Space-Efficient Error Reduction for Unitary Quantum Computations

Bill Fefferman* Hirotada Kobayashi† Cedric Yen-Yu Lin* Tomoyuki Morimae‡
Harumichi Nishimura§

*Joint Center for Quantum Information and Computer Science
University of Maryland
College Park, MD, USA

†Principles of Informatics Research Division
National Institute of Informatics
Tokyo, Japan

‡Advanced Scientific Research Leaders Development Unit
Gunma University
Kiryu, Gunma, Japan

§Department of Computer Science and Mathematical Informatics
Graduate School of Information Science
Nagoya University
Nagoya, Aichi, Japan

27 April 2016

Abstract

This paper develops general space-efficient methods for error reduction for unitary quantum computation. Consider a polynomial-time quantum computation with completeness c and soundness s, either with or without a witness (corresponding to QMA and BQP, respectively). To convert this computation into a new computation with error at most 2^{-p}, the most space-efficient method known requires extra workspace of $O\bigl(p \log \frac{1}{c-s}\bigr)$ qubits. This space requirement is too large for scenarios like logarithmic-space quantum computations. This paper presents error-reduction methods for unitary quantum computations (i.e., computations without intermediate measurements) that require extra workspace of just $O\bigl(\log \frac{p}{c-s}\bigr)$ qubits. This in particular gives the first methods of strong amplification for logarithmic-space unitary quantum computations with two-sided bounded error. This also leads to a number of consequences in complexity theory, such as the uselessness of quantum witnesses in bounded-error logarithmic-space unitary quantum computations, the PSPACE upper bound for QMA with exponentially-small completeness-soundness gap, and strong amplification for matchgate computations.

1 Introduction

1.1 Background

A very basic topic in various models of quantum computation is whether computation error can be efficiently reduced within a given model. For polynomial-time bounded error quantum computation, the most standard model of quantum computation, the computation error can be made exponentially small via a simple repetition followed by a threshold-value decision. This justifies the choice of $2/3$ and $1/3$ for the completeness and soundness parameters in the definition of the corresponding complexity class BQP. This is also the case for quantum Merlin-Arthur (QMA) proof systems, another central model of quantum computation that models a quantum analogue of NP (more precisely, MA), and the resulting class QMA may again be defined with completeness and soundness parameters $2/3$ and $1/3$.

An undesirable feature of the simple repetition-based error reduction above is that the necessary workspace enlarges linearly with respect to the number of repetitions. More explicitly, for a given p, the number of repetitions necessary to achieve an error of 2^{-p} is $O\bigl(\frac{p}{(c-s)^2}\bigr)$, and thus both the workspace size and the witness size become $O\bigl(\frac{p}{(c-s)^2}\bigr)$ times larger. This implies that the simple repetition-based method is no longer useful when either the workspace size or the witness size is required to be logarithmically bounded.

Marriott and Watrous [MW05] developed a more sophisticated method of error reduction for QMA proof systems that does not increase the witness size at all. For a given p, their method still requires $O\bigl(\frac{p}{(c-s)^2}\bigr)$ calls of the original computation and its inverse to achieve the computation error 2^{-p}, but the method reuses both the workspace and the witness every time it calls the original computation and its inverse. Hence, the witness size never increases in their method. This is a strong property that allows them to show the uselessness of logarithmic-size quantum witnesses in QMA proof systems (i.e., $\mathrm{QMA}_{\log} = \mathrm{BQP}$, where $\mathrm{QMA}_{\log}$ is the class of problems having QMA proof systems with logarithmic-size quantum witnesses). Their method is also more efficient in workspace size than the simple repetition-based method, but still requires extra workspace of size $O\bigl(\frac{p}{(c-s)^2}\bigr)$, as it must record outcomes of all the calls of the original computation and its inverse.

Nagaj, Wocjan, and Zhang [NWZ09] succeeded in reducing to $O\bigl(\frac{p}{c-s}\bigr)$ the number of calls of the original computation and its inverse necessary to achieve the computation error 2^{-p} for a given p, while keeping the witness size unchanged. Their method makes use of the phase-estimation algorithm, an essential component of many quantum algorithms including the celebrated factoring algorithm. To achieve error 2^{-p} for a given p, their method must repeat $O(p)$ times the phase-estimation algorithm with precision of at least $O\bigl(\log \frac{1}{c-s}\bigr)$ bits and record all these estimated phases. Hence, this phase-estimation-based method uses extra workspace of size $O\bigl(p \log \frac{1}{c-s}\bigr)$.

As can be seen from above, both of the Marriott-Watrous method and the phase-estimation-based method are still insufficient for the case where the workspace size must be logarithmically bounded. No efficient error-reduction method is known that keeps the size of additionally necessary workspace logarithmically bounded. This is not limited to the case of QMA proof systems, and in fact almost no efficient error-reduction method is known even in the case of logarithmic-space quantum computations, and in the case of space-bounded quantum computations in general. The study of general space-bounded quantum computations was initiated by Watrous [Wat99] based on quantum Turing machines. Several models of space-bounded quantum computations have been proposed and investigated since then in the literature [Wat01, Wat03, Wat09a, JKMW10, vMW12, TS13], some considering only logarithmic-space quantum computations and others treating general cases. It is not known whether any of these models are computationally equivalent. It is also not known whether error reduction is possible for logarithmic-space quantum computation defined according to any of these models, except the only known affirmative answer shown by Watrous [Wat01] on computation of one-sided bounded error performed by logarithmic-space quantum Turing machines. As negative evidence in the case where computational resources are too limited, computation error cannot be reduced below a certain constant for one-way quantum finite state automata [AF98].

1.2 Main Result and Its Consequences

This paper presents a general method of strong and space-efficient error reduction for *unitary* quantum computations. In particular, the method is applicable to logarithmic-space unitary quantum computations and logarithmic-space unitary QMA proof systems. All the results in this paper are model-independent and hold with any model of space-bounded quantum computations as long as it performs *unitary* quantum computations. The unitary model is not the most general in that it does not allow any intermediate measurements (notice that the standard technique of simulating intermediate measurements by unitary gates requires unallowably many ancilla qubits in the case of space-bounded computations), but is arguably one of the most reasonable models of space-bounded quantum computation.

Let $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of positive and nonnegative integers, respectively. Let $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s)$ denote the class of problems having QMA proof systems with completeness c and soundness s, where the verifier performs a *unitary* quantum computation that has no time bound but is restricted to use $l_{\mathsf{V}}(n)$ private qubits and to receive a quantum witness of $l_{\mathsf{M}}(n)$ qubits on every input of length n. The main result of this paper is the following strong and space-efficient error-reduction for such QMA-type computations.

Theorem 1. *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and for any functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$ satisfying $c > s$, there exists a function $\delta \colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}](1 - 2^{-p}, 2^{-p}).$$

This paper presents three different proofs of this main theorem, all of which are based on reductions that are in space logarithmic and also in time polynomial with respect to $\frac{p}{c-s}$. As will be found in Section 5, the theorem can be proved by remarkably simple arguments. Nevertheless, the theorem is very powerful in that it fruitfully leads to many consequences that substantially deepen the understanding on the power of QMA proof systems and quantum computations in general, both in the space-bounded scenario and in the usual polynomial-time scenario. In what follows, a function $f \colon \mathbb{Z}^+ \to \mathbb{N}$ is *polynomially bounded* if f is polynomial-time computable and $f(n)$ is in $O(n^d)$ for some constant $d > 0$, and is *logarithmically bounded* if f is logarithmic-space computable and $f(n)$ is in $O(\log n)$.

Strong amplification for unitary BQL The first consequence of Theorem 1 is a remarkably strong error-reducibility in logarithmic-space unitary quantum computations. Let $\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c, s)$ denote the class of problems solvable by logarithmic-space unitary quantum computations with completeness c and soundness s. The following amplifiability is immediate from Theorem 1 by taking a function p to be logarithmic-space computable and polynomially bounded, functions c and s to be logarithmic-space computable and to satisfy $c - s \geq 1/q$ for some polynomially bounded function $q \colon \mathbb{Z}^+ \to \mathbb{N}$, a function l_{V} to be logarithmically bounded, and a function $l_{\mathsf{M}} = 0$.

Corollary 2. *For any polynomially bounded function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic-space computable and for any logarithmic-space computable functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q \colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c, s) \subseteq \mathrm{Q}_{\mathbf{U}}\mathrm{L}(1 - 2^{-p}, 2^{-p}).$$

This in particular justifies defining the bounded-error class $\mathrm{BQ}_{\mathbf{U}}\mathrm{L}$ of logarithmic-space unitary quantum computations by $\mathrm{BQ}_{\mathbf{U}}\mathrm{L} = \mathrm{Q}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$, employing $2/3$ and $1/3$ for completeness and soundness parameters. Before this work, Watrous [Wat01] showed a similar strong error-reducibility in the case of one-sided bounded error, and Corollary 2 extends this to the two-sided bounded error case.

Uselessness of quantum witnesses in logarithmic-space unitary QMA Let $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s)$ denote the class of problems having logarithmic-space unitary QMA proof systems (i.e., such systems in which a verifier performs a logarithmic-space unitary computation upon receiving a logarithmic-size quantum witness) with completeness c and soundness s. Similarly to Corollary 2, the following amplifiability is immediate from Theorem 1 by taking a function p to be logarithmic-space computable and polynomially bounded, functions c and s to be logarithmic-space computable and to satisfy $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, and functions l_{V} and l_{M} to be logarithmically bounded.

Corollary 3. *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic-space computable and for any logarithmic-space computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{L}(1-2^{-p}, 2^{-p}).$$

Again this justifies defining the bounded-error class $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}$ of logarithmic-space unitary QMA proof systems by $\mathrm{QMA}_{\mathbf{U}}\mathrm{L} = \mathrm{QMA}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$. By a standard technique of replacing a quantum witness by a totally mixed state as a self-prepared witness (to do this in a unitary computation, one can simply prepare sufficiently many EPR pairs and then take a qubit from each pair), Corollary 3 together with Corollary 2 further implies the equivalence of $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}$ and $\mathrm{BQ}_{\mathbf{U}}\mathrm{L}$.

Corollary 4. $\mathrm{QMA}_{\mathbf{U}}\mathrm{L} = \mathrm{BQ}_{\mathbf{U}}\mathrm{L}$.

As mentioned before, Marriott and Watrous [MW05] showed the equivalence $\mathrm{QMA}_{\log} = \mathrm{BQP}$, the uselessness of quantum witnesses of logarithmic size in the standard QMA proof systems with a polynomial-time verifier. In this respect, Corollary 4 states that quantum witnesses of logarithmic size do not increase the power of logarithmic-space unitary quantum computations at all, and indeed extends the result of Marriott and Watrous to logarithmic-space case.

Space-efficient amplification for QMA Let $\mathrm{QMA}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$ be the time-efficient version of $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, i.e., the class of problems having standard polynomial-time QMA proof systems with completeness c and soundness s in which a polynomial-time unitary quantum verifier receives a quantum witness of $l_{\mathsf{M}}(n)$ qubits and uses workspace of $l_{\mathsf{V}}(n)$ qubits on every input of length n. As the reduction is in time polynomial with respect to $\frac{p}{c-s}$ in the proof of Theorem 1, the following amplifiability is immediate from Theorem 1 by taking functions p, l_{V}, and l_{M} to be polynomially bounded, and functions c and s to be polynomial-time computable and to satisfy $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$.

Corollary 5. *For any polynomially bounded functions $p, l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and for any polynomial-time computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s) \subseteq \mathrm{QMA}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}](1-2^{-p}, 2^{-p}).$$

Recall that the Marriott-Watrous amplification [MW05] requires δ to be in $O\bigl(\frac{p}{(c-s)^2}\bigr)$ and the phase-estimation-based method by Nagaj, Wocjan, and Zhang [NWZ09] requires δ to be in $O\bigl(p \log \frac{1}{c-s}\bigr)$, instead of δ in $O\bigl(\log \frac{p}{c-s}\bigr)$ of Corollary 5. Hence, the methods in this paper are most space-efficient among known error-reduction methods for standard QMA proof systems, and also among those for BQP.

Strong amplification for unitary QMAPSPACE Let $\mathrm{Q_{\mathbf{U}}PSPACE}(c,s)$ denote the class of problems solvable by polynomial-space unitary quantum computations with completeness c and soundness s, and let $\mathrm{QMA_{\mathbf{U}}PSPACE}(c,s)$ denote the class of problems having polynomial-space unitary QMA proof systems (i.e., such systems in which a verifier performs a polynomial-space unitary computation upon receiving a polynomial-size quantum witness) with completeness c and soundness s. The following corollary states the scaled-up versions of Corollaries 2 and 3, and again is immediate from Theorem 1 by taking a function p to be polynomial-space computable and exponentially bounded, functions c and s to be polynomial-space computable and to satisfy $c-s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, and functions l_{V} and l_{M} to be polynomially bounded (or a function $l_{\mathsf{M}} = 0$ in the case of $\mathrm{Q_{\mathbf{U}}PSPACE}(c,s)$).

Corollary 6. *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and for any polynomial-space computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c-s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, the following two properties hold:*

(i) $\mathrm{Q_{\mathbf{U}}PSPACE}(c,s) \subseteq \mathrm{Q_{\mathbf{U}}PSPACE}\bigl(1-2^{-2^p}, 2^{-2^p}\bigr)$.

(ii) $\mathrm{QMA_{\mathbf{U}}PSPACE}(c,s) \subseteq \mathrm{QMA_{\mathbf{U}}PSPACE}\bigl(1-2^{-2^p}, 2^{-2^p}\bigr)$.

Again by a standard technique of replacing a quantum witness by a totally mixed state as a self-prepared witness, the following corollary follows from Corollary 6 together with the fact that $\mathrm{RevPSPACE} = \mathrm{PrQPSPACE} = \mathrm{PSPACE}$ [Ben89, Wat99], where $\mathrm{RevPSPACE}$ and $\mathrm{PrQPSPACE}$ are the complexity classes corresponding to deterministic polynomial-space reversible computations and unbounded-error polynomial-space quantum computations, respectively.

Corollary 7. *For any polynomial-space computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c-s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{QMA_{\mathbf{U}}PSPACE}(c,s) = \mathrm{PSPACE}.$$

Now the PSPACE upper bound immediately follows for the class of problems having standard polynomial-time QMA proof systems with exponentially small completeness-soundness gap. More precisely, for the class $\mathrm{QMA}(c,s)$ of problems having standard polynomial-time QMA proof systems with completeness c and soundness s, the following corollary holds.

Corollary 8. *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and for any polynomial-time computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c-s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{QMA}(c,s) \subseteq \mathrm{PSPACE}.$$

For QMA proof systems with exponentially small completeness-soundness gap, the PSPACE upper bound was known previously only for the one-sided-error case (following from the result in Ref. [IKW12]), and only the EXP upper bound was known for the two-sided-error case (following from the result in Ref. [KW00]). Natarajan and Wu [NW16] independently proved a statement equivalent to Corollary 8. In fact, statements equivalent to Corollary 8 were also proved with different proofs independently by the first and third authors of the present paper in Ref. [FL16a] (see Ref. [FL16b] also) and by the complement subset of the present authors. The first and third authors of the present paper further proved in Refs. [FL16a, FL16b] that the converse of Corollary 8 also holds, i.e., PSPACE is characterized by QMA proof systems with exponentially small completeness-soundness gap.

Strong amplification for matchgate computations A matchgate is defined to be a two-qubit gate of the form $G(A, B)$ corresponding to the four-by-four unitary matrix in which the four corner elements form A and the four inner-square elements form B for matrices A and B in $\mathrm{SU}(2)$, and all the other elements are 0. A matchgate circuit is a quantum circuit such that: (i) the input state is a computational basis state, (ii) all the gates of the circuit are matchgates which are applied to two neighbor qubits, and (iii) the output is a final measurement in the computational basis on any single qubit. Matchgate computations were introduced and proved classically simulable by Valiant [Val02]. Terhal and DiVincenzo [TD02] related them to noninteracting-fermion quantum circuits. Let $\mathrm{MG}(c, s)$ denote the class of problems solvable by polynomial-time matchgate computations with completeness c and soundness s. Using the equivalence of polynomial-time matchgate computations and logarithmic-space unitary computations shown by Jozsa, Kraus, Miyake, and Watrous [JKMW10, Corollary 3.3], the following is immediate from Corollary 2.

Corollary 9. *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic-space computable and for any logarithmic-space computable functions $c, s\colon \mathbb{Z}^+ \to [0, 1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{MG}(c, s) \subseteq \mathrm{MG}(1 - 2^{-p}, 2^{-p}).$$

1.3 Roadmap

We assume familiarity with basic quantum formalism (see Refs. [NC00, KSV02, Wil13], for instance).

Section 2 provides outlines of three different proofs of the main theorem. Subsection 2.1 overviews the simplest construction among the three, which is based on phase estimation. Subsection 2.2 then briefly explains a hybrid construction based on both phase estimation and the Marriott-Watrous amplification, which is most efficient among the three in terms of the number of calls of the original unitary transformation of the verifier. Subsection 2.3 sketches an alternative construction based on random guess, which is exactly implementable when the Hadamard and any classical reversible transformations are exactly implementable. Section 3 presents precise definitions of the model of space-bounded unitary quantum Merlin-Arthur proof systems and associated complexity classes. Section 4 describes several procedures that are used in the main error-reduction procedures of this paper. Finally, Section 5 provides the three proofs of the main theorem rigorously.

2 Overview of Proofs

This section provides outlines of the three different proofs of the main theorem. Consider any unitary transformation V_x of the verifier on input x, and let p_{acc} be the maximum acceptance probability of it (and thus, $p_{\mathrm{acc}} \geq c(|x|)$ for yes instances, and $p_{\mathrm{acc}} \leq s(|x|)$ for no instances).

2.1 Simple Construction Based on Phase Estimation

The first construction of space-efficient amplification is very simple and mainly based on phase estimation. The key idea is to first use phase estimation so that it just reduces computation error *mildly* to be polynomially small rather than directly to be exponentially small. The point is that the phase estimation is performed only once rather than multiple times. By essentially taking the AND of the polynomially many attempts of this mildly amplified procedure, one then achieves exponentially small soundness with keeping sufficiently large completeness (say, $1/2$). Finally, one makes completeness exponentially close to one while keeping exponentially small soundness, which is done by essentially taking the OR of the polynomially many attempts of the procedure constructed so far.

More precisely, let $\mathcal{H}$ be the Hilbert space over which V_x acts, and let $I_{\mathcal{H}}$ be the identity operator over $\mathcal{H}$. Further let Π_{init} be the projection onto the subspace spanned by the legal initial states of the QMA-type computation induced by V_x, and let Π_{acc} be the projection onto the subspace spanned by the accepting states of the QMA-type computation associated with V_x. Consider the unitary operator $Q_x = \bigl(2V_x^\dagger \Pi_{\mathrm{acc}} V_x - I_{\mathcal{H}}\bigr)\bigl(2\Pi_{\mathrm{init}} - I_{\mathcal{H}}\bigr)$ corresponding to one iteration of the Grover-type algorithm induced by V_x. First, one performs one-shot phase estimation associated with Q_x with $l(|x|)$-bit precision for a function $l \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $l = \bigl\lceil \log \frac{2\pi}{\arccos \sqrt{s} - \arccos \sqrt{c}} \bigr\rceil$ and with *mild* failure probability $\frac{1}{q_1(|x|)}$, where q_1 is a function in $O(p)$ (precisely speaking, $q_1 = 2(p + \lceil \log(p+2) \rceil) + 4$). From the property of the standard phase-estimation algorithm, the number of additional qubits used by the resulting procedure is determined by the function $l + \bigl\lceil \log(\frac{q_1}{2} + 2) \bigr\rceil$, which is at most linear in $\log \frac{p}{c-s}$ (in fact, at most $\log \frac{p}{c-s}$ plus a constant). The acceptance probability is *mildly* amplified to at least $1 - \frac{1}{q_1(|x|)}$ in the yes-instance case, while it is *mildly* reduced to at most $\frac{1}{q_1(|x|)}$ in the no-instance case.

Let $V_x^{(1)}$ be the unitary operator corresponding to the procedure constructed so far. Now repeat the following procedure $N_1(|x|)$ times for $N_1 = \bigl\lceil \frac{q_2}{2 \log q_1} \bigr\rceil$, where q_2 is also a function in $O(p)$ (precisely speaking, $q_2 = p + \lceil \log(p+2) \rceil$ so that $q_1 = 2q_2 + 4$): One applies $V_x^{(1)}$, and then increments a counter by 1 if the state corresponds to a rejection state of it. One further applies $\bigl(V_x^{(1)}\bigr)^\dagger$, the inverse of $V_x^{(1)}$, and then increments a counter by one if any of the work qubits of $V_x^{(1)}$ is in state $|1\rangle$. After the repetition, one accepts if and only if the counter value remains zero. Intuitively, these repetitions try to take the AND of the $N_1(|x|)$ attempts of $V_x^{(1)}$ (with some suitable initialization try by $\bigl(V_x^{(1)}\bigr)^\dagger$). The rigorous analysis shows that the initialization steps also contribute to taking AND, so that this process is exactly equivalent to taking the AND of $2\,N_1(|x|)$ attempts of $V_x^{(1)}$. The number of additional qubits used by the resulting procedure is $O(\log N_1)$, which is clearly at most linear in $\log \frac{p}{c-s}$. The acceptance probability is thus reduced to at most $\bigl(\frac{1}{q_1(|x|)}\bigr)^{2\,N_1(|x|)} \leq 2^{-\,q_2(|x|)}$ in the no-instance case, while it is still at least $1 - \frac{2\,N_1(|x|)}{q_1(|x|)} > \frac{1}{2}$ in the yes-instance case.

Let $V_x^{(2)}$ be the unitary operator corresponding to the procedure constructed so far. Finally, one tries to take the OR of $2\,N_2(|x|)$ attempts of $V_x^{(2)}$ for a function $N_2 \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $N_2 = \lceil \frac{p}{2} \rceil$, which is done by performing a repetition similar to above. The number of additional qubits used by the resulting procedure is $O(\log N_2)$, which is clearly at most linear in $\log \frac{p}{c-s}$. The acceptance probability is amplified to at least $1 - 2^{-\,p(|x|)}$ in the yes-instance case, while it is still at most $2\,N_2(|x|) \cdot 2^{-\,q_2(|x|)} < 2^{-\,p(|x|)}$ in the no-instance case, as desired.

2.2 Hybrid Construction of Phase Estimation and Marriott-Watrous

Recall that the necessary number of calls of the (controlled) unitary transformation U is $2^l \cdot \bigl\lceil \frac{1}{2\varepsilon} + 2 \bigr\rceil - 1$ for a phase estimation associated with U precise to l bits with failure probability ε [NC00]. Hence, a straightforward calculation shows that the simple construction in the last subsection requires $O\bigl(\frac{1}{c-s} \cdot \frac{p^3}{\log p}\bigr)$ calls of V_x and its inverse. This subsection presents an idea to construct a more efficient method that uses $O\bigl(\frac{1}{c-s} \cdot \frac{p^2}{\log p}\bigr)$ calls of V_x and its inverse. The idea here is to use phase estimation so that it just achieves a *very mild* computation error of some constant, rather than polynomially small. One then achieves polynomially small error by the Marriott-Watrous amplification. The rest of the construction is essentially the same as in the simple construction in the last subsection.

More precisely, the construction first performs one-shot phase estimation with $l(|x|)$-bit precision for a function $l \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $l = \bigl\lceil \log \frac{2\pi}{\arccos \sqrt{s} - \arccos \sqrt{c}} \bigr\rceil$ and with *very mild* failure probability $\frac{1}{4}$. From the property of the standard phase-estimation algorithm, the number of additional qubits used by the resulting procedure is determined by the function $l + 2$, which is at most $\log \frac{1}{c-s}$ plus a constant, and thus, clearly at most linear in $\log \frac{p}{c-s}$ when the final targeted computation error is at most 2^{-p} for a function $p \colon \mathbb{Z}^+ \to \mathbb{N}$. The acceptance probability is *very mildly* amplified to at least $\frac{3}{4}$ in the yes-instance case, while it is *very mildly* reduced to at most $\frac{1}{4}$ in the no-instance case.

Let $V_x^{(1)}$ be the unitary operator corresponding to the procedure constructed so far. Next, one further reduces computation error still mildly to be polynomially small by performing the Marriott-Watrous amplification. By using $N_1(|x|)$ calls of $V_x^{(1)}$ and its inverse for a function $N_1 : \mathbb{Z}^+ \to \mathbb{N}$ defined by $N_1 = \lceil \frac{8 \log(2p)}{\log e} \rceil$, the acceptance probability is *mildly* amplified to at least $1 - \frac{1}{4(p(|x|))^2}$ in the yes-instance case, while it is *mildly* reduced to at most $\frac{1}{4(p(|x|))^2}$ in the no-instance case. The number of additional qubits used by the resulting procedure is determined by the function $2N_1 + \lceil \log(2N_1 + 1) \rceil + 1$, which is clearly at most linear in $\log p$ (and thus, at most linear in $\log \frac{p}{c-s}$ also).

Let $V_x^{(2)}$ be the unitary operator corresponding to the procedure constructed so far. The rest of the construction is essentially the same as in the last subsection. One can essentially take the AND of $2\, N_2(|x|)$ attempts of $V_x^{(2)}$ for a function $N_2 : \mathbb{Z}^+ \to \mathbb{N}$ defined by $N_2 = \lceil \frac{p}{2 \log(2p)} \rceil$ to achieve acceptance probability at least $1 - \frac{1}{p(|x|)}$ for yes instances and at most $2^{-2\, p(|x|)}$ for no instances. Let $V_x^{(3)}$ be the resulting unitary operator. One then essentially takes the OR of $2\, N_3(|x|)$ attempts of $V_x^{(3)}$ for a function $N_3 : \mathbb{Z}^+ \to \mathbb{N}$ defined by $N_3 = \lceil \frac{p}{2 \log p} \rceil$ to achieve acceptance probability at least $1 - 2^{-\, p(|x|)}$ for yes instances and at most $2^{-\, p(|x|)}$ for no instances.

The total number of additional qubits required is clearly determined by a function at most linear in $\log \frac{p}{c-s}$. A straightforward calculation shows that this construction uses $O\bigl(\frac{1}{c-s} \cdot \frac{p^2}{\log p}\bigr)$ calls of V_x and its inverse, as claimed.

2.3 Exactly Implementable Construction Based on a Random Guess

One small drawback of the previous two constructions is that they are not exactly implementable when implemented by quantum circuits with any gate set of finite size, due to the use of the phase-estimation algorithm. This subsection outlines an alternative construction that is exactly implementable when the Hadamard and any classical reversible transformations are exactly implementable. The construction uses $O\Bigl(\frac{1}{(c-s)^3} \cdot p^{\frac{5}{2}} + \frac{1}{(c-s)^3} \bigl(\log \frac{1}{c-s}\bigr)^{\frac{3}{2}} \cdot p\Bigr)$ calls of V_x and its inverse, which is not so good as the second construction in Subsection 2.2, but is at least incomparable with the simple construction in Subsection 2.1.

The idea is to guess p_{acc} with *mild* precision of $l(|x|)$ bits, where $l : \mathbb{Z}^+ \to \mathbb{N}$ is the function defined by $l = \lceil \frac{1}{2} \log \frac{6q}{(c-s)^2} \rceil$ for a function $q : \mathbb{Z}^+ \to \mathbb{N}$ defined by $q = \lceil 2\bigl(p + \log \frac{6p}{c-s} + 1\bigr) \rceil$ when the final targeted computation error is at most 2^{-p} for a function $p : \mathbb{Z}^+ \to \mathbb{N}$. For each j in $\{1, \ldots, 2^{l(|x|)}\}$, let $r_j = j \cdot 2^{-\, l(|x|)}$ be a possible guess of p_{acc}. Pick an integer k from $\{1, \ldots, 2^{l(|x|)}\}$ uniformly at random, and reject immediately if $r_k = k \cdot 2^{-\, l(|x|)} < c(|x|)$ (so that no k can result in a good guess at p_{acc} for no instances). Otherwise r_k is used as a guess at p_{acc}. The point is that, for yes instances, there exists a choice of k such that $|r_k - p_{\mathrm{acc}}| < 2^{-\, l(|x|)} \leq \sqrt{\frac{(c(|x|) - s(|x|))^2}{6\, p(|x|)}}$, while for no instances, it holds that $|r_k - p_{\mathrm{acc}}| > c(|x|) - s(|x|)$ for any choice of k. Hence, by first applying the additive adjustment of acceptance probability [JKNN12] to obtain the unitary transformation $V_{x,k}^{(1)}$ from V_x, and then performing Reflection Procedure [KLGN15] using $V_{x,k}^{(1)}$, the acceptance probability can be *mildly* amplified to at least $1 - \frac{(c(|x|) - s(|x|))^2}{6\, q(|x|)}$ in the yes-instance case, if the chosen k corresponds to the appropriate guess r_k, while the acceptance probability is at most $1 - \bigl(c(|x|) - s(|x|)\bigr)^2$ for any guess r_k.

Fix an index k of the guess r_k and let $V_{x,k}^{(2)}$ be the unitary operator corresponding to the procedure constructed so far. As in the previous subsections, one tries to essentially take the AND of $2\, N_2(|x|)$ attempts of $V_{x,k}^{(2)}$ for a function $N_2 : \mathbb{Z}^+ \to \mathbb{N}$ defined by $N_2 = \lceil \frac{q}{2(c-s)^2} \rceil$. The acceptance probability is still at least $\frac{1}{2}$ in the yes-instance case when the appropriate guess r_k at p_{acc} is made, while it is at most $e^{-\, q(|x|)} < 2^{-\, q(|x|)}$ for any guess r_k in the no-instance case.

Let $V_{x,k}^{(3)}$ be the unitary operator corresponding to the procedure constructed so far, when the index k of r_k

is chosen. Taking into account that k is chosen uniformly at random, the above argument results in a unitary transformation $V_x^{(4)}$ that has acceptance probability at least $2^{-l(|x|)} \cdot \frac{1}{2} > \frac{1}{4}\sqrt{\frac{(c(|x|)-s(|x|))^2}{6\,q(|x|)}}$ in the yes-instance case and at most $2^{-q(|x|)} \leq 2^{-\frac{q(|x|)}{2}} \cdot \bigl(\frac{c(|x|)-s(|x|)}{12\,p(|x|)}\bigr) \cdot 2^{-p(|x|)}$ in the no-instance case.

Finally, as in the previous subsections, one tries to essentially take the OR of $2\,N_4(|x|)$ attempts of $V_x^{(4)}$ for a function $N_4 \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $N_4 = \left\lceil 2\sqrt{\frac{6q}{(c-s)^2}} \cdot p \right\rceil$. The acceptance probability is amplified to at least $1 - 2^{-p(|x|)}$ in the yes-instance case, and is at most $2^{-p(|x|)}$ for any guess r_k in the no-instance case.

3 Space-Bounded Unitary Quantum Merlin-Arthur Proof Systems

First we summarize some notations that are used in this paper. Let $\Sigma = \{0,1\}$ denote the binary alphabet set. In this paper, all Hilbert spaces are complex and of dimension a power of two. For a Hilbert space $\mathcal{H}$, let $I_{\mathcal{H}}$ denote the identity operator over $\mathcal{H}$. A quantum register is a set of single or multiple qubits. For a quantum register R, let I_{R} denote the identity operator over the Hilbert space associated with R.

A *space-bounded unitary quantum Merlin-Arthur (QMA) proof system*, or simply called a *QMA-type computation* throughout this paper, is a space-bounded unitary quantum computation performed by a *quantum verifier* V. As in the standard QMA proof system, V prepares a quantum register V corresponding to his/her private space, all the qubits of which are initially in state $|0\rangle$, and receives a quantum register M storing an arbitrarily prepared quantum witness. One of the qubit in V is designated as the output qubit of V, which without loss of generality is assumed to be the first qubit of V. V performs a unitary quantum computation over (V, M) and then measures the output qubit in the computational basis, where the measurement outcome 1 corresponds to acceptance. On an input x in Σ^*, the number of private qubits in V and the length of a quantum witness in M are restricted to $l_{\mathsf{V}}(|x|)$ and $l_{\mathsf{M}}(|x|)$ according to some predetermined functions l_{V} and l_{M} that depend only on the input length $|x|$. Unless explicitly mentioned, no restriction is put on the time complexity of the unitary quantum computation of V.

Formally, for functions $l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$, an $(l_{\mathsf{V}}, l_{\mathsf{M}})$*-space-bounded quantum verifier V for a space-bounded unitary quantum Merlin-Arthur proof system* is a machine that on an input x in Σ^* performs a unitary transformation V_x, where each V_x acts over $l_{\mathsf{V}}(|x|) + l_{\mathsf{M}}(|x|)$ qubits, the first $l_{\mathsf{V}}(|x|)$ qubits of which correspond to the register V and the rest $l_{\mathsf{M}}(|x|)$ qubits of which correspond to the register M. It is assumed that such a machine V corresponds to a certain reasonable l-space-bounded unitary quantum computation model for some function $l \colon \mathbb{Z}^+ \to \mathbb{N}$ such that $l(n)$ is in $O(l_{\mathsf{V}}(n) + l_{\mathsf{M}}(n))$. For instance, V may be an l-space classical-quantum hybrid Turing machine [Wat03, Wat09a] for unitary quantum computations, or may be a machine that first runs a classical Turing machine of an l-space uniformly generated family of unitary quantum circuits and then performs the generated circuit. It is stressed that all the results in this paper hold regardless of the models of space-bounded quantum computations as long as the computations performed are unitary.

Fix an input x in Σ^*, and suppose that V receives a quantum witness ρ of $l_{\mathsf{M}}(|x|)$ qubits in M. The probability $p_{\mathrm{acc}}(V_x, \rho)$ that V accepts x with a quantum witness ρ is given by

$$p_{\mathrm{acc}}(V_x, \rho) = \operatorname{tr} \Pi_{\mathrm{acc}} V_x^{\dagger} \bigl[(|0\rangle\langle 0|)^{\otimes l_{\mathsf{V}}(|x|)} \otimes \rho\bigr] V_x,$$

where $\Pi_{\mathrm{acc}} = |1\rangle\langle 1| \otimes I^{\otimes(l_{\mathsf{V}}(|x|)+l_{\mathsf{M}}(|x|)-1)}$ is the projection onto the subspace spanned by the states in which the designated output qubit is in state $|1\rangle$.

The class $\mathrm{QMA_U SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$ of problems having $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded unitary QMA systems is defined as follows.

Definition 10. Given functions $l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, a promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in $\mathrm{QMA_U SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$ if there exists an $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier V for a space-bounded unitary quantum Merlin-Arthur proof system such that, for every x in Σ^*, (Completeness) if x is in A_{yes}, there exists a quantum witness ρ of $l_{\mathsf{M}}(|x|)$ qubits that makes V accept x with probability at least $c(|x|)$, and

(Soundness) if x is in A_{no}, for any quantum witness ρ of $l_{\mathsf{M}}(|x|)$ qubits, V accepts x with probability at most $s(|x|)$.

Note that quantum witnesses may be restricted to pure states, as allowing quantum witnesses of mixed states does not increase the maximal accepting probability of proof systems.

The classes $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s)$ and $\mathrm{QMA}_{\mathbf{U}}\mathrm{PSPACE}(c,s)$ corresponding to the logarithmic-space and polynomial-space QMA-type computations, respectively, with completeness c and soundness s are then obtained by restricting both of the functions l_{V} and l_{M} in Definition 10 to be logarithmically bounded and polynomially bounded.

Definition 11. Given functions $c,s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s)$ iff A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$ for some logarithmically bounded functions $l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$.

Definition 12. Given functions $c,s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{PSPACE}(c,s)$ iff A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$ for some polynomially bounded functions $l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$.

When $l_{\mathsf{M}} = 0$ in Definitions 11 and 12, respectively, the resulting classes $\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c,s)$ and $\mathrm{Q}_{\mathbf{U}}\mathrm{PSPACE}(c,s)$ correspond to the standard logarithmic-space and polynomial-space unitary quantum computations with completeness c and soundness s.

Definition 13. Given functions $c,s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c,s)$ iff A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, 0](c,s)$ for some logarithmically bounded function $l_{\mathsf{V}}\colon \mathbb{Z}^+ \to \mathbb{N}$.

Definition 14. Given functions $c,s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathrm{Q}_{\mathbf{U}}\mathrm{PSPACE}(c,s)$ iff A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, 0](c,s)$ for some polynomially bounded function $l_{\mathsf{V}}\colon \mathbb{Z}^+ \to \mathbb{N}$.

Finally, the bounded-error classes $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}$ and $\mathrm{BQ}_{\mathbf{U}}\mathrm{L}$ may be defined as follows.

Definition 15. A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}$ iff A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$.

Definition 16. A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathrm{BQ}_{\mathbf{U}}\mathrm{L}$ iff A is in $\mathrm{Q}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$.

4 Basic Procedures

Let $\mathcal{H}$ be any Hilbert space of dimension a power of two. Given a unitary transformation U and two projections Δ and Π, all acting over $\mathcal{H}$, define the Hermitian operator M over $\mathcal{H}$ by

$$M = \Delta U^{\dagger} \Pi U \Delta,$$

which plays crucial roles in many well-known amplification methods in quantum computation, including the Grover search [Gro96], the Marriott-Watrous amplification for QMA [MW05], the Nagaj-Wocjan-Zhang amplification for QMA based on phase estimation [NWZ09], and quantum rewinding for zero-knowledge proofs against quantum attacks [Wat09b].

ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $(U, \Delta, \Pi, t, l, \varepsilon)$

1. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. Let Q be the unitary transformation defined by $Q = (2U^\dagger \Pi U - I_{\mathsf{Q}})(2\Delta - I_{\mathsf{Q}})$. Perform the phase estimation associated with Q acting over the state in Q with precision of l bits and failure probability ε, using $l + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ ancilla qubits. Accept if the estimated phase is in the interval $(-t, t)$ and reject otherwise.

Figure 1: The ONE-SHOT PHASE-ESTIMATION PROCEDURE.

ONE-SHOT PHASE-ESTIMATION PROCEDURE Consider the procedure described in Figure 1, which is at the core of the amplification method based on phase estimation proposed by Nagaj, Wocjan, and Zhang [NWZ09]. The following proposition holds with the ONE-SHOT PHASE-ESTIMATION PROCEDURE.

Proposition 17 ([NWZ09])**.** *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space. Let ε be a real number in $(0,1)$, let l be a positive integer, and let t be a real number in $\left[0, \frac{1}{2}\right]$ represented by l bits. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ satisfying that $\frac{1}{\pi} \arccos \sqrt{\lambda} \leq t$. Then, the* ONE-SHOT PHASE-ESTIMATION PROCEDURE *associated with $(U, \Delta, \Pi, t, l, \varepsilon)$ results in acceptance with probability $1 - \varepsilon$ when the state $|\phi_\lambda\rangle$ is received in register* Q *in Step 1.*

(Soundness) *Suppose that all the eigenvalues λ of M are such that $\frac{1}{\pi} \arccos \sqrt{\lambda} \geq t + 2^{-l}$. Then, the* ONE-SHOT PHASE-ESTIMATION PROCEDURE *associated with $(U, \Delta, \Pi, t, l, \varepsilon)$ results in acceptance with probability at most ε regardless of the quantum state received in register* Q *in Step 1.*

Remark. One thing to be mentioned is that the standard phase-estimation algorithm involves inverting quantum Fourier transformation, which cannot be implemented exactly when implemented by quantum circuits with a gate set of finite size. Thus, one needs to approximately implement some phase-rotation gates. The number of phase-rotation gates necessary to approximate is proportional to l^2 to achieve precision of l bits in the standard implementation of a phase-estimation algorithm. This means that each phase-rotation gate must be approximated within $O\left(\frac{\varepsilon}{l^2}\right)$ so that approximate implementation does not significantly affect the failure probability ε of the phase-estimation algorithm. To prove Theorem 1 via the simple construction based on phase estimation, one needs to perform a phase-estimation algorithm with precision l at least logarithmic with respect to $\frac{p}{c-s}$ and with failure probability ε at most polynomially small with respect to p. The standard (constructive) proofs of the Solovay-Kitaev theorem [Kit97] (such as those found in Refs. [NC00, KSV02, DN06]) require space polylogarithmic with respect to $\frac{1}{\delta}$ when approximating within δ, which is insufficient for the purpose of proving Theorem 1 via the simple construction based on phase estimation. Fortunately, van Melkebeek and Watson [vMW12] showed a more space-efficient construction of the Solovay-Kitaev approximation, which uses space only logarithmic with respect to $\frac{1}{\delta}$ and can be used for the simple construction based on phase estimation to prove Theorem 1.

AND-TYPE REPETITION PROCEDURE Given a unitary transformation U and two projections Δ and Π all acting over a Hilbert space, consider the process of applying U to a fixed initial state $|\phi\rangle$ in a quantum register Q that is in the subspace corresponding to Δ and then accepting if and only if the resulting state is projected onto the subspace corresponding to Π by the projective measurement $\{\Pi, I_{\mathsf{Q}} - \Pi\}$. Let p denote the accepting probability of this process. By running N independent attempts of such a process, the probability clearly becomes p^N for the event that all the attempts result in acceptance, but which requires N copies of the initial state $|\phi\rangle$. When $|\phi\rangle$ is

AND-Type Repetition Procedure associated with (U, Δ, Π, N)

1. Let $l = \lceil \log(2N+1) \rceil$, and prepare an l-qubit register C, where all the qubits in C are initialized to state $|0\rangle$. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. For $j = 1$ to N, perform the following:
   - 2.1. Apply U to Q.
   - 2.2. If the state in Q belongs to the subspace corresponding to the projection $I_{\mathsf{Q}} - \Pi$, apply $U_{+1}(\mathbb{Z}_{2^l})$ to C, where $U_{+1}(\mathbb{Z}_{2^l})$ is the unitary transformation defined by
   $$U_{+1}(\mathbb{Z}_{2^l})\colon |j\rangle \mapsto \big|(j+1) \bmod 2^l\big\rangle, \quad \forall j \in \mathbb{Z}_{2^l}.$$
   - 2.3. Apply $U^\dagger$ to Q.
   - 2.4. If the state in Q belongs to the subspace corresponding to the projection $I_{\mathsf{Q}} - \Delta$, apply $U_{+1}(\mathbb{Z}_{2^l})$ to C.
3. Accept if the content of C is 0 (i.e., all the qubits in C are in state $|0\rangle$), and reject otherwise.

Figure 2: The AND-Type Repetition Procedure.

an eigenstate of the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$, the following AND-Type Repetition Procedure essentially simulates such independent attempts with just one copy of $|\phi\rangle$.

Prepare an l-qubit register C that serves as a counter modulo 2^l, where $l = \lceil \log(2N+1) \rceil$. All the qubits in C are initialized to state $|0\rangle$. The procedure receives a quantum register Q that contains a state in the subspace corresponding to Δ, and then repeats N times a pair of a simulation attempt by U and an initialization attempt by $U^\dagger$. After each attempt of applying U to Q, the procedure checks if the state in Q belongs to the subspace corresponding to Π, and increments the counter in C if this check fails. Similarly, after each attempt of applying $U^\dagger$ to Q, it checks if the state in Q is back to a legal initial state belonging to the subspace corresponding to Δ, and increments the counter in C if this check fails. After the repetition, the procedure accepts if and only if the counter in C is still 0. Figure 2 presents the precise description of the AND-Type Repetition Procedure.

The following proposition holds with the AND-Type Repetition Procedure.

Proposition 18. *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space, and let N be a positive integer. For the* AND-Type Repetition Procedure *associated with (U, Δ, Π, N), let U' be the unitary transformation induced by it, let Δ' be the projection onto the subspace spanned by the legal initial states of it, and let Π' be the projection onto the subspace spanned by the accepting states of it. Suppose that the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$ has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then the state $|\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}$ is an eigenstate of the Hermitian operator $M' = \Delta'(U')^\dagger \Pi' U' \Delta'$ with eigenvalue λ^{2N}.*

Proof. The unitary transformation U' can be written as

$$U' = \big\{ \big[\Delta \otimes I_{\mathsf{C}} + (I_{\mathsf{Q}} - \Delta) \otimes U_{+1}(\mathbb{Z}_{2^l})\big] (U^\dagger \otimes I_{\mathsf{C}}) \big[\Pi \otimes I_{\mathsf{C}} + (I_{\mathsf{Q}} - \Pi) \otimes U_{+1}(\mathbb{Z}_{2^l})\big] (U \otimes I_{\mathsf{C}}) \big\}^N,$$

whereas the projections Δ' and Π' can be written as

$$\Delta' = \Delta \otimes (|0\rangle\langle 0|)^{\otimes l}, \quad \Pi' = I_{\mathsf{Q}} \otimes (|0\rangle\langle 0|)^{\otimes l}.$$

Notice that, for any k in $\{1, \ldots, 2N\}$, it holds that

$$(|0\rangle\langle 0|)^{\otimes l} \big(U_{+1}(\mathbb{Z}_{2^l})\big)^k (|0\rangle\langle 0|)^{\otimes l} = 0,$$

since the content of C, which starts at 0, cannot return to 0 for k applications of the increment transformation $U_{+1}(\mathbb{Z}_{2^l})$, for $k \leq 2N < 2^l$. This implies that M' can be simply written as

$$M' = \Delta'(U')^\dagger \Pi' U' \Delta' = \big[\Delta\big[(\Delta U^\dagger \Pi U)^\dagger\big]^N (\Delta U^\dagger \Pi U)^N \Delta\big] \otimes (|0\rangle\langle 0|)^{\otimes l} = M^{2N} \otimes (|0\rangle\langle 0|)^{\otimes l}.$$

Hence, if $|\phi_\lambda\rangle$ is an eigenstate of M with eigenvalue λ, then $|\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}$ is an eigenstate of M' with eigenvalue λ^{2N}. $\square$

Now the following property of the AND-TYPE REPETITION PROCEDURE is immediate from Proposition 18.

Proposition 19. *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space, and let N be a positive integer. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* AND-TYPE REPETITION PROCEDURE *associated with (U, Δ, Π, N) results in acceptance with probability λ^{2N} when the state $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

(Soundness) *Suppose that all the eigenvalues of M are at most ε for some ε in $[0, 1)$. Then, the* AND-TYPE REPETITION PROCEDURE *associated with (U, Δ, Π, N) results in acceptance with probability at most ε^{2N} regardless of the quantum state received in register Q in Step 1.*

OR-TYPE REPETITION PROCEDURE One can also construct a procedure that essentially simulates the process of taking OR of the N independent attempts mentioned before with just one copy of $|\phi\rangle$. One now applies $U_{+1}(\mathbb{Z}_{2^l})$ to C when the state in Q belongs to the subspace corresponding to the projection Π at Step 2.2 of the AND-TYPE REPETITION PROCEDURE, and *rejects* if and only if the content of C is 0 at Step 3 of the AND-TYPE REPETITION PROCEDURE. The resulting procedure is called the OR-TYPE REPETITION PROCEDURE, whose precise description is presented in Figure 3.

Similarly to the AND-TYPE REPETITION PROCEDURE, the following proposition holds with the OR-TYPE REPETITION PROCEDURE.

Proposition 20. *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space, and let N be a positive integer. For the* OR-TYPE REPETITION PROCEDURE *associated with (U, Δ, Π, N), let U' be the unitary transformation induced by it, let Δ' be the projection onto the subspace spanned by the legal initial states of it, and let Π' be the projection onto the subspace spanned by the accepting states of it. Suppose that the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$ has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then the state $|\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}$ is an eigenstate of the Hermitian operator $M' = \Delta'(U')^\dagger \Pi' U' \Delta'$ with eigenvalue $1 - (1 - \lambda)^{2N}$.*

Proof. The proof is very similar to the proof of Proposition 18. This time, the unitary transformation U' can be written as

$$U' = \big\{\big[\Delta \otimes I_{\mathsf{C}} + (I_{\mathsf{Q}} - \Delta) \otimes U_{+1}(\mathbb{Z}_{2^l})\big](U^\dagger \otimes I_{\mathsf{C}})\big[\Pi \otimes U_{+1}(\mathbb{Z}_{2^l}) + (I_{\mathsf{Q}} - \Pi) \otimes I_{\mathsf{C}}\big](U \otimes I_{\mathsf{C}})\big\}^N,$$

whereas the projections Δ' and Π' can be written as

$$\Delta' = \Delta \otimes (|0\rangle\langle 0|)^{\otimes l}, \quad \Pi' = I_{\mathsf{Q}} \otimes \big[I_{\mathsf{C}} - (|0\rangle\langle 0|)^{\otimes l}\big].$$

OR-TYPE REPETITION PROCEDURE associated with (U, Δ, Π, N)

1. Let $l = \lceil \log(2N+1) \rceil$, and prepare an l-qubit register C, where all the qubits in C are initialized to state $|0\rangle$. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. For $j = 1$ to N, perform the following:
   - 2.1. Apply U to Q.
   - 2.2. If the state in Q belongs to the subspace corresponding to the projection Π, apply $U_{+1}(\mathbb{Z}_{2^l})$ to C, where $U_{+1}(\mathbb{Z}_{2^l})$ is the unitary transformation defined by
   $$U_{+1}(\mathbb{Z}_{2^l}) \colon |j\rangle \mapsto \bigl|(j+1) \bmod 2^l\bigr\rangle, \quad \forall j \in \mathbb{Z}_{2^l}.$$
   - 2.3. Apply $U^\dagger$ to Q.
   - 2.4. If the state in Q belongs to the subspace corresponding to the projection $I_{\mathsf{Q}} - \Delta$, apply $U_{+1}(\mathbb{Z}_{2^l})$ to C.
3. Reject if the content of C is 0 (i.e., all the qubits in C are in state $|0\rangle$), and accept otherwise.

Figure 3: The OR-TYPE REPETITION PROCEDURE.

Again notice that, for any k in $\{1, \ldots, 2N\}$, it holds that

$$(|0\rangle\langle 0|)^{\otimes l} \bigl(U_{+1}(\mathbb{Z}_{2^l})\bigr)^k (|0\rangle\langle 0|)^{\otimes l} = 0,$$

and thus, M' can be simply written as

$$\begin{aligned} M' &= \Delta' - \Delta'(U')^\dagger (I_{(\mathsf{Q},\mathsf{C})} - \Pi')U'\Delta' \\ &= \bigl\{\Delta - \Delta\bigl[(\Delta U^\dagger (I_{\mathsf{Q}} - \Pi)U)^\dagger\bigr]^N \bigl[\Delta U^\dagger (I_{\mathsf{Q}} - \Pi)U\bigr]^N \Delta\bigr\} \otimes (|0\rangle\langle 0|)^{\otimes l} \\ &= \bigl[\Delta - (\Delta - M)^{2N}\bigr] \otimes (|0\rangle\langle 0|)^{\otimes l}. \end{aligned}$$

Now notice that $\lambda|\phi_\lambda\rangle = M|\phi_\lambda\rangle = \Delta M|\phi_\lambda\rangle = \lambda\Delta|\phi_\lambda\rangle$, and therefore at least one of $\Delta|\phi_\lambda\rangle = |\phi_\lambda\rangle$ or $\lambda = 0$ holds. If $\Delta|\phi_\lambda\rangle = |\phi_\lambda\rangle$, it obviously holds that

$$M'\bigl(|\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}\bigr) = \bigl[1 - (1-\lambda)^{2N}\bigr]\bigl(|\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}\bigr).$$

On the other hand, when $\lambda = 0$, by using that $M\Delta = \Delta M = M$ and $M|\phi_\lambda\rangle = 0$, it follows that

$$M'\bigl(|\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}\bigr) = \bigl(\Delta - \Delta^{2N}\bigr)\bigl(|\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}\bigr) = 0,$$

which is sufficient for the claim, because $1 - (1-\lambda)^{2N} = 0$ in this case. □

Now the following property of the OR-TYPE REPETITION PROCEDURE is immediate from Proposition 20.

Proposition 21. *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space, and let N be a positive integer. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* OR-TYPE REPETITION PROCEDURE *associated with (U, Δ, Π, N) results in acceptance with probability $1 - (1-\lambda)^{2N}$ when the state $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

MARRIOTT-WATROUS AMPLIFICATION PROCEDURE associated with (U, Δ, Π, N, t)

1. Let $l = \lceil \log(2N+1) \rceil$. Prepare a single-qubit register B_j for each j in $\{0, \ldots, 2N\}$, and an l-qubit register C, where all the qubits in B_j and C are initialized to state $|0\rangle$. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. For $j = 1$ to N, perform the following:
   - 2.1. Apply U to Q.
   - 2.2. If the state in Q belongs to the subspace corresponding to the projection $I_{\mathsf{Q}} - \Pi$, apply the Pauli transformation X (i.e., the NOT transformation) to B_j.
   - 2.3. Apply $U^\dagger$ to Q.
   - 2.4. If the state in Q belongs to the subspace corresponding to the projection $I_{\mathsf{Q}} - \Delta$, apply X to B_{j+1}.
3. For $j = 1$ to $2N$, perform the following:
   If the content of B_j is the same as that of B_{j-1}, apply $U_{+1}(\mathbb{Z}_{2^l})$ to C, where $U_{+1}(\mathbb{Z}_{2^l})$ is the unitary transformation defined by
   $$U_{+1}(\mathbb{Z}_{2^l})\colon |j\rangle \mapsto \left|(j+1) \bmod 2^l\right\rangle, \quad \forall j \in \mathbb{Z}_{2^l}.$$
4. Accept if the content of C is at least t (when viewed as an integer in $\mathbb{Z}_{2^l}$), and reject otherwise.

Figure 4: The MARRIOTT-WATROUS AMPLIFICATION PROCEDURE.

(Soundness) *Suppose that all the eigenvalues of M are at most ε for some ε in $[0, 1)$. Then, the* OR-TYPE REPETITION PROCEDURE *associated with (U, Δ, Π, N) results in acceptance with probability at most $1 - (1-\varepsilon)^{2N}$ regardless of the quantum state received in register Q in Step 1.*

MARRIOTT-WATROUS AMPLIFICATION PROCEDURE Consider the procedure described in Figure 4, which is exactly the amplification method (described in a general form) proposed by Marriott and Watrous [MW05].

The following proposition holds with the MARRIOTT-WATROUS AMPLIFICATION PROCEDURE.

Proposition 22 ([MW05]). *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space. Let N and t be positive integers satisfying $t \leq 2N$. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue $\lambda \geq \frac{t}{2N} + \varepsilon$ for some ε in $\left(0, 1 - \frac{t}{2N}\right]$. Then, the* MARRIOTT-WATROUS AMPLIFICATION PROCEDURE *associated with (U, Δ, Π, N, t) results in acceptance with probability greater than $1 - e^{-4\varepsilon^2 N}$ when the state $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

(Soundness) *Suppose that all the eigenvalues of M are at most $\frac{t}{2N} - \varepsilon$ for some ε in $\left(0, \frac{t}{2N}\right]$. Then, the* MARRIOTT-WATROUS AMPLIFICATION PROCEDURE *associated with (U, Δ, Π, N, t) results in acceptance with probability less than $e^{-4\varepsilon^2 N}$ regardless of the quantum state received in register Q in Step 1.*

ADDITIVE ADJUSTMENT PROCEDURE associated with (U, Δ, Π, l, k)

1. Prepare a single-qubit register B and an l-qubit register R, where all the qubits in B and R are initialized to state $|0\rangle$. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. Apply the Hadamard transformation H to each qubit in (B, R), and apply U to Q.
3. Accept either if B contains 0 *and* the state in Q belongs to the subspace corresponding to Π or if B contains 1 *and* the content of R is greater than k (when viewed as an integer in $\{1, \ldots, 2^l\}$), and reject otherwise.

Figure 5: The ADDITIVE ADJUSTMENT PROCEDURE.

ADDITIVE ADJUSTMENT PROCEDURE For a Hilbert space $\mathcal{H}_j$ for each j in $\{1, 2\}$, consider a unitary transformation U_j and two projections Δ_j and Π_j, all acting over $\mathcal{H}_j$. Define the Hermitian operator M_j over $\mathcal{H}_j$ for each j in $\{1, 2\}$ by $M_j = \Delta_j U_j^\dagger \Pi_j U_j \Delta_j$.

Now define a Hilbert space $\mathcal{H}'$ defined by $\mathcal{H}' = \mathcal{B} \otimes \mathcal{H}_1 \otimes \mathcal{H}_2$, where $\mathcal{B} = \mathbb{C}(\Sigma)$ is a Hilbert space corresponding to a single qubit. Let

$$\Delta' = |0\rangle\langle 0| \otimes \Delta_1 \otimes \Delta_2, \quad \Pi' = |0\rangle\langle 0| \otimes \Pi_1 \otimes I_{\mathcal{H}_2} + |1\rangle\langle 1| \otimes I_{\mathcal{H}_1} \otimes \Pi_2, \quad U' = H \otimes U_1 \otimes U_2,$$

where H denotes the Hadamard transformation, and further let $M' = \Delta'(U')^\dagger \Pi' U' \Delta'$. A straightforward calculation shows that

$$M' = \frac{1}{2}(|0\rangle\langle 0| \otimes M_1 \otimes \Delta_1 + |0\rangle\langle 0| \otimes \Delta_2 \otimes M_2).$$

Suppose that, for each j in $\{1, 2\}$, the Hermitian operator M_j has an eigenstate (i.e., the normalized eigenvector) $|\phi_{j,\lambda_j}\rangle$ with its associated eigenvalue λ_j. It is easy to see that

$$M'(|0\rangle \otimes |\phi_{1,\lambda_1}\rangle \otimes |\phi_{2,\lambda_2}\rangle) = \frac{\lambda_1 + \lambda_2}{2}(|0\rangle \otimes |\phi_{1,\lambda_1}\rangle \otimes |\phi_{2,\lambda_2}\rangle).$$

This implies that M' has an eigenstate $|0\rangle \otimes |\phi_{1,\lambda_1}\rangle \otimes |\phi_{2,\lambda_2}\rangle$ with eigenvalue $\frac{\lambda_1+\lambda_2}{2}$, which is implicit in the additive adjustment technique of acceptance probability proposed in Ref. [JKNN12]. This leads to the following ADDITIVE ADJUSTMENT PROCEDURE presented in Figure 5.

The following proposition is immediate from the argument above.

Proposition 23. *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space, and let l be a positive integer and k be an integer in $\{1, \ldots, 2^l\}$. For the* ADDITIVE ADJUSTMENT PROCEDURE *associated with (U, Δ, Π, l, k), let U' be the unitary transformation induced by it, let Δ' be the projection onto the subspace spanned by the legal initial states of it, and let Π' be the projection onto the subspace spanned by the accepting states of it. Suppose that the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$ has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then the state $|0\rangle \otimes |\phi_\lambda\rangle \otimes |0\rangle^{\otimes l}$ is an eigenstate of the Hermitian operator $M' = \Delta'(U')^\dagger \Pi' U' \Delta'$ with eigenvalue $\frac{1}{2} + \frac{1}{2}\big(\lambda - \frac{k}{2^l}\big)$.*

Now the following property of the ADDITIVE ADJUSTMENT PROCEDURE is immediate from Proposition 23.

Proposition 24. *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. For any positive integer l and any integer k in $\{1, \ldots, 2^l\}$, the following two properties hold:*

REFLECTION PROCEDURE associated with (U, Δ, Π)

1. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. Apply U to Q.
3. Perform a phase-flip (i.e., multiply the phase by -1) if the state in Q belongs to the subspace corresponding to the projection Π.
4. Apply $U^\dagger$ to Q.
5. Reject if the state in Q belongs to the subspace corresponding to Δ, and accept otherwise.

Figure 6: The REFLECTION PROCEDURE.

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* ADDITIVE ADJUSTMENT PROCEDURE *associated with (U, Δ, Π, l, k) results in acceptance with probability $\frac{1}{2} + \frac{1}{2}\left(\lambda - \frac{k}{2^l}\right)$ when the state $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

(Soundness) *Suppose that all the eigenvalues of M are at most ε for some ε in $[0, 1)$. Then, the* ADDITIVE ADJUSTMENT PROCEDURE *associated with (U, Δ, Π, l, k) results in acceptance with probability at most $\frac{1}{2} + \frac{1}{2}\left(\varepsilon - \frac{k}{2^l}\right)$ regardless of the quantum state received in register Q in Step 1.*

REFLECTION PROCEDURE Finally, consider the procedure described in Figure 6, which is exactly the REFLECTION PROCEDURE in a general form originally developed in Ref. [KLGN15].

The following proposition holds with the REFLECTION PROCEDURE.

Proposition 25 ([KLGN15])**.** *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* REFLECTION PROCEDURE *associated with (U, Δ, Π) results in acceptance with probability $4\lambda(1-\lambda)$ when the state $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

(Soundness) *Suppose that none of the eigenvalues of M is in the interval $\left(\frac{1}{2} - \varepsilon, \frac{1}{2} + \varepsilon\right)$ for some ε in $\left(0, \frac{1}{2}\right]$. Then, the* REFLECTION PROCEDURE *associated with (U, Δ, Π) results in acceptance with probability at most $1 - 4\varepsilon^2$ regardless of the quantum state received in register Q in Step 1.*

5 Space-Efficient Amplification Methods

This section rigorously proves Theorem 1 in the three different ways.

Throughout this section, consider any QMA-type computation for a problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ induced by a family $\{V_x\}_{x \in \Sigma^*}$ of a unitary transformation V_x of the verifier on input x in Σ^* that acts over a quantum register $\mathsf{Q} = (\mathsf{V}, \mathsf{M})$, where V is the quantum register consisting of all the private qubits of the verifier, and M is the one for storing a received quantum witness. Let Π_{init} be the projection onto the subspace spanned by the legal initial states of the QMA-type computation induced by V_x (i.e., the subspace spanned by those in which all the qubits in V is in state $|0\rangle$) and let Π_{acc} be the projection onto the subspace spanned by the accepting states of the QMA-type

MILD AMPLIFICATION WITH PHASE ESTIMATION associated with (V_x, p)

Define a function $l\colon \mathbb{Z}^+ \to \mathbb{N}$ by $l = \left\lceil \log \frac{2\pi}{\arccos\sqrt{s} - \arccos\sqrt{c}} \right\rceil$ and let $t\colon \mathbb{Z}^+ \to \left[0, \frac{1}{2}\right]$ be a function such that, for every nonnegative integer n, $t(n)$ is an approximation of $\frac{1}{2\pi}\left(\arccos\sqrt{c(n)} + \arccos\sqrt{s(n)}\right)$ with $l(n)$-bit precision. Let Π_{init} and Π_{acc} be the projections onto the subspaces spanned by the legal initial states and the accepting states, respectively, in the verification with V_x.

Perform the ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $\left(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}}, t(|x|), l(|x|), \frac{1}{p(|x|)}\right)$.

Figure 7: The MILD AMPLIFICATION WITH PHASE ESTIMATION.

computation associated with V_x (i.e., the subspace spanned by states for which the designated output qubit of V_x is in state $|0\rangle$). The maximum eigenvalue of the Hermitian operator $M_x = \Pi_{\mathrm{init}} V_x^\dagger \Pi_{\mathrm{acc}} V_x \Pi_{\mathrm{init}}$ exactly corresponds to the maximum acceptance probability of the verifier on input x over all possible quantum witnesses received in M. Hence, M_x has an eigenvalue at least $c(|x|)$ if x is in A_{yes}, while all eigenvalues of M_x are at most $s(|x|)$ if x is in A_{no}, where $c, s\colon \mathbb{Z}^+ \to [0,1]$ are functions that provide completeness and soundness conditions of the QMA-type computation induced by $\{V_x\}_{x\in\Sigma^*}$, respectively.

5.1 Simple Construction Based on Phase Estimation

The first proof is via the simple construction based on phase estimation.

Mild amplification with a phase estimation Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, arbitrarily. Let $l\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$l = \left\lceil \log \frac{2\pi}{\arccos\sqrt{s} - \arccos\sqrt{c}} \right\rceil,$$

and let $t\colon \mathbb{Z}^+ \to \left[0, \frac{1}{2}\right]$ be a function such that, for every nonnegative integer n, $t(n)$ is an approximation of $\frac{1}{2\pi}\left(\arccos\sqrt{c(n)} + \arccos\sqrt{s(n)}\right)$ with $l(n)$-bit precision.

Fix an input x. Given the triplet $(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}})$, one constructs the ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $\left(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}}, t(|x|), l(|x|), \frac{1}{p(|x|)}\right)$. The resulting procedure is called the MILD AMPLIFICATION WITH PHASE ESTIMATION, and is summarized in Figure 7.

The following lemma is proved by using the MILD AMPLIFICATION WITH PHASE ESTIMATION combined with the properties of the ONE-SHOT PHASE-ESTIMATION PROCEDURE stated in Proposition 17.

Lemma 26. *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and any functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}]\left(1 - \frac{1}{p}, \frac{1}{p}\right).$$

Proof. Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x\in\Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and an input x in Σ^*. Consider the ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $\left(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}}, t(|x|), l(|x|), \frac{1}{p(|x|)}\right)$, which is exactly what the MILD AMPLIFICATION WITH PHASE ESTIMATION associated with (V_x, p) performs.

SOUNDNESS ERROR REDUCTION associated with (V_x, p)

Define a function $N\colon \mathbb{Z}^+ \to \mathbb{N}$ by $N = \left\lceil \frac{p}{2\log(2p+4)} \right\rceil$. Consider the MILD AMPLIFICATION WITH PHASE ESTIMATION associated with $(V_x, 2p+4)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.
Perform the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\bigr)$.

Figure 8: The SOUNDNESS ERROR REDUCTION.

From Proposition 17, it holds that, if x is in A_{yes}, the ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $\bigl(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}}, t(|x|), l(|x|), \frac{1}{p(|x|)}\bigr)$ results in acceptance with probability at least $1 - \frac{1}{p(|x|)}$, while if x is in A_{no}, it results in acceptance with probability at most $\frac{1}{p(|x|)}$, which shows the completeness and soundness.

The ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $\bigl(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}}, t(|x|), l(|x|), \frac{1}{p(|x|)}\bigr)$ uses extra workspace of $\delta(|x|) = l(|x|) + \left\lceil \log\bigl(\frac{p(|x|)}{2} + 2\bigr) \right\rceil$ qubits. As is proved in Ref [NWZ09], the function $l = \left\lceil \log \frac{2\pi}{\arccos\sqrt{s} - \arccos\sqrt{c}} \right\rceil$ is logarithmic with respect to $\frac{1}{c-s}$, and thus, the used extra workspace is logarithmic with respect to $\frac{p}{c-s}$, as claimed. $\square$

Soundness error-reduction Again fix arbitrarily a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $N\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$N = \left\lceil \frac{p}{2\log(2p+4)} \right\rceil.$$

Fix an input x. Given the pair (V_x, p), consider the MILD AMPLIFICATION WITH PHASE ESTIMATION associated with $(V_x, 2p+4)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it. From the triplet $\bigl(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}\bigr)$ and a positive integer $N(|x|)$, one constructs the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\bigr)$, and performs it. The resulting procedure is called the SOUNDNESS ERROR REDUCTION, and is summarized in Figure 8.

The following lemma is proved by using the SOUNDNESS ERROR REDUCTION combined with the properties of the MILD AMPLIFICATION WITH PHASE ESTIMATION used for proving Lemma 26.

Lemma 27. *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and any functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}]\left(\frac{1}{2}, 2^{-p}\right).$$

Proof. Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and an input x in Σ^*. The lemma is proved by considering the SOUNDNESS ERROR REDUCTION associated with (V_x, p).

First consider the MILD AMPLIFICATION WITH PHASE ESTIMATION associated with $(V_x, 2p+4)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.

Lemma 26 and its proof ensure that A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta_1, l_{\mathsf{M}}]\big(1 - \frac{1}{2p+4}, \frac{1}{2p+4}\big)$ for some function $\delta_1 \colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$, and this inclusion is certified by the MILD AMPLIFICATION WITH PHASE ESTIMATION associated with $(V_x, 2p+4)$. This in particular implies that the Hermitian operator $M'_x = \Pi'_{\mathrm{init}}(V'_x)^\dagger \Pi'_{\mathrm{acc}} V'_x \Pi'_{\mathrm{init}}$ has an eigenvalue at least $1 - \frac{1}{2\,p(|x|)+4}$ if x is in A_{yes}, while all the eigenvalues of M'_x are at most $\frac{1}{2\,p(|x|)+4}$ if x is in A_{no}.

Now consider the AND-TYPE REPETITION PROCEDURE associated with $\big(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\big)$, which is exactly what the SOUNDNESS ERROR REDUCTION associated with (V_x, p) performs. By Proposition 19, the AND-TYPE REPETITION PROCEDURE associated with $\big(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\big)$ results in acceptance with probability at least

$$\left(1 - \frac{1}{2\,p(|x|)+4}\right)^{2\,N(|x|)} > \left(1 - \frac{1}{2\,p(|x|)+4}\right)^{p(|x|)+2} > \frac{1}{2}$$

if x is in A_{yes}, and at most

$$\left(\frac{1}{2\,p(|x|)+4}\right)^{2\,N(|x|)} \leq \left(2^{-\log(2\,p(|x|)+4)}\right)^{\frac{p(|x|)}{\log(2\,p(|x|)+4)}} = 2^{-\,p(|x|)}$$

if x is in A_{no}, and the completeness and soundness follows.

The AND-TYPE REPETITION PROCEDURE associated with $\big(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\big)$ uses extra workspace (relative to V'_x) of $\delta_2(|x|)$ qubits for the function $\delta_2 \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $\delta_2 = \lceil \log(2N+1) \rceil$. As $N = \big\lceil \frac{p}{2\log(2p+4)} \big\rceil$, δ_2 is clearly logarithmic with respect to p, and thus, with respect to $\frac{p}{c-s}$ also. Hence, the SOUNDNESS ERROR REDUCTION associated with (V_x, p) uses extra workspace (relative to V_x) of logarithmically many qubits with respect to $\frac{p}{c-s}$ also (which is determined by a function $\delta = \delta_1 + \delta_2$), as desired. $\square$

Space-efficient error reduction based on phase estimation Again fix arbitrarily a function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $N \colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$N = \left\lceil \frac{p}{2} \right\rceil.$$

Fix an input x. Given the pair (V_x, p), consider the SOUNDNESS ERROR REDUCTION associated with $\big(V_x, p + \lceil \log(p+2) \rceil\big)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it. From the triplet $\big(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}\big)$ and a positive integer $N(|x|)$, one constructs the OR-TYPE REPETITION PROCEDURE associated with $\big(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\big)$, and performs it. The resulting procedure is called the SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION, and is summarized in Figure 9.

Now Theorem 1, the main theorem of this paper, is ready to be proved by using the SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION combined with the properties of the SOUNDNESS ERROR REDUCTION used for proving Lemma 27.

Proof of Theorem 1 (via the simple construction based on phase estimation). Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and an input x in Σ^*. The theorem is proved by considering the SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION associated with (V_x, p).

First consider the SOUNDNESS ERROR REDUCTION associated with $\big(V_x, p + \lceil \log(p+2) \rceil\big)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.

SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION associated with (V_x, p)

Define a function $N\colon \mathbb{Z}^+ \to \mathbb{N}$ by $N = \lceil \frac{p}{2} \rceil$. Consider the SOUNDNESS ERROR REDUCTION associated with $\bigl(V_x, p + \lceil \log(p+2) \rceil\bigr)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.
Perform the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$.

Figure 9: The SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION.

Lemma 27 and its proof ensure that A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta_1, l_{\mathsf{M}}]\bigl(\frac{1}{2}, \frac{1}{p+2} \cdot 2^{-p}\bigr)$ for some function $\delta_1\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$, and this inclusion is certified by the SOUNDNESS ERROR REDUCTION associated with $\bigl(V_x, p + \lceil \log(p+2) \rceil\bigr)$. This in particular implies that the Hermitian operator $M'_x = \Pi'_{\mathrm{init}} (V'_x)^\dagger \Pi'_{\mathrm{acc}} V'_x \Pi'_{\mathrm{init}}$ has an eigenvalue at least $\frac{1}{2}$ if x is in A_{yes}, while all the eigenvalues of M'_x are at most $\frac{1}{p(|x|)+2} \cdot 2^{-p(|x|)}$ if x is in A_{no}.

Now consider the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$, which is exactly what the SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION associated with (V_x, p) performs. By Proposition 21, the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$ results in acceptance with probability at least

$$1 - \left(1 - \frac{1}{2}\right)^{2\,N(|x|)} \geq 1 - 2^{-\,p(|x|)}$$

if x is in A_{yes}, and at most

$$1 - \left(1 - \frac{1}{p(|x|)+2} \cdot 2^{-\,p(|x|)}\right)^{2\,N(|x|)} < 1 - \left(1 - \frac{1}{p(|x|)+2} \cdot 2^{-\,p(|x|)}\right)^{p(|x|)+2} < 2^{-\,p(|x|)}$$

if x is in A_{no}, and the completeness and soundness follows.

The OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$ uses extra workspace (relative to V'_x) of $\delta_2(|x|)$ qubits for the function $\delta_2\colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $\delta_2 = \lceil \log(2N+1) \rceil$. As $N = \lceil \frac{p}{2} \rceil$, δ_2 is clearly logarithmic with respect to p, and thus, with respect to $\frac{p}{c-s}$ also. Hence, the SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION associated with (V_x, p) uses extra workspace (relative to V_x) of logarithmically many qubits with respect to $\frac{p}{c-s}$ also (which is determined by a function $\delta = \delta_1 + \delta_2$), as desired. ☐

Recall that the necessary number of calls of the (controlled) unitary transformation U is $2^l \cdot \lceil \frac{1}{2\varepsilon} + 2 \rceil - 1$ for a phase estimation associated with U precise to l bits with failure probability ε [NC00]. Hence, a straightforward calculation shows that the SPACE-EFFICIENT ERROR REDUCTION BASED ON PHASE ESTIMATION associated with (V_x, p) uses $O\bigl(\frac{1}{c-s} \cdot \frac{p^3}{\log p}\bigr)$ calls of V_x and its inverse.

5.2 Hybrid construction of phase estimation and Marriott-Watrous

The second proof is based on the hybrid construction of phase estimation and Marriott-Watrous.

Very mild amplification with a phase estimation Fix functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, arbitrarily. Again let $l\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$l = \left\lceil \log \frac{2\pi}{\arccos \sqrt{s} - \arccos \sqrt{c}} \right\rceil,$$

VERY MILD AMPLIFICATION WITH PHASE ESTIMATION associated with V_x

Define a function $l\colon \mathbb{Z}^+ \to \mathbb{N}$ by $l = \left\lceil \log \frac{2\pi}{\arccos\sqrt{s} - \arccos\sqrt{c}} \right\rceil$ and let $t\colon \mathbb{Z}^+ \to \left[0, \frac{1}{2}\right]$ be a function such that, for every nonnegative integer n, $t(n)$ is an approximation of $\frac{1}{2\pi}\left(\arccos\sqrt{c(n)} + \arccos\sqrt{s(n)}\right)$ with $l(n)$-bit precision. Let Π_{init} and Π_{acc} be the projections onto the subspaces spanned by the legal initial states and the accepting states, respectively, in the verification with V_x.

Perform the ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $\left(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}}, t(|x|), l(|x|), \frac{1}{4}\right)$.

Figure 10: The VERY MILD AMPLIFICATION WITH PHASE ESTIMATION.

and let $t\colon \mathbb{Z}^+ \to \left[0, \frac{1}{2}\right]$ be a function such that, for every nonnegative integer n, $t(n)$ is an approximation of $\frac{1}{2\pi}\left(\arccos\sqrt{c(n)} + \arccos\sqrt{s(n)}\right)$ with $l(n)$-bit precision.

Fix an input x. Given the triplet $(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}})$, one constructs the ONE-SHOT PHASE-ESTIMATION PROCEDURE associated with $\left(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}}, t(|x|), l(|x|), \frac{1}{4}\right)$. The resulting procedure is called the VERY MILD AMPLIFICATION WITH PHASE ESTIMATION, and is summarized in Figure 10.

In fact, the VERY MILD AMPLIFICATION WITH PHASE ESTIMATION associated with V_x is nothing but the MILD AMPLIFICATION WITH PHASE ESTIMATION associated with $(V_x, 4)$. Hence, the following lemma is immediate by using the VERY MILD AMPLIFICATION WITH PHASE ESTIMATION combined with Lemma 26 and its proof.

Lemma 28. *For any functions $l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and any functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{1}{c-s}$ such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}]\left(\frac{3}{4}, \frac{1}{4}\right).$$

Mild amplification with Marriott-Watrous Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, arbitrarily. Let $N\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$N = \left\lceil \frac{4\log p}{\log e} \right\rceil.$$

Fix an input x. Given the pair (V_x, p), consider the VERY MILD AMPLIFICATION WITH PHASE ESTIMATION associated with V_x. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it. From the triplet $\left(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}\right)$ and a positive integer $N(|x|)$, one constructs the MARRIOTT-WATROUS AMPLIFICATION PROCEDURE associated with $\left(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\right)$, and performs it. The resulting procedure is called the MILD AMPLIFICATION WITH MARRIOTT-WATROUS, and is summarized in Figure 11.

Now Lemma 26 is alternatively proved by using the MILD AMPLIFICATION WITH MARRIOTT-WATROUS combined with the properties of the MARRIOTT-WATROUS AMPLIFICATION PROCEDURE stated in Proposition 22.

Proof of Lemma 26 (via the hybrid construction of phase estimation and Marriott-Watrous) . Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x\in\Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and an input x in Σ^*. The lemma is proved by considering the MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with (V_x, p).

MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with (V_x, p)

Define a function $N\colon \mathbb{Z}^+ \to \mathbb{N}$ by $N = \lceil \frac{4 \log p}{\log e} \rceil$. Consider the VERY MILD AMPLIFICATION WITH PHASE ESTIMATION associated with V_x. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.

Perform the MARRIOTT-WATROUS AMPLIFICATION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|), N(|x|)\bigr)$.

Figure 11: The MILD AMPLIFICATION WITH MARRIOTT-WATROUS.

First consider the VERY MILD AMPLIFICATION WITH PHASE ESTIMATION associated with V_x. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.

Lemma 28 and its proof ensure that A is in $\mathrm{QMA_U SPACE}[l_{\mathsf{V}} + \delta_1, l_{\mathsf{M}}]\bigl(\frac{3}{4}, \frac{1}{4}\bigr)$ for some function $\delta_1\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{1}{c-s}$, and this inclusion is certified by the VERY MILD AMPLIFICATION WITH PHASE ESTIMATION associated with V_x. This in particular implies that the Hermitian operator $M'_x = \Pi'_{\mathrm{init}}(V'_x)^\dagger \Pi'_{\mathrm{acc}} V'_x \Pi'_{\mathrm{init}}$ has an eigenvalue at least $\frac{3}{4}$ if x is in A_{yes}, while all the eigenvalues of M'_x are at most $\frac{1}{4}$ if x is in A_{no}.

Now consider the MARRIOTT-WATROUS AMPLIFICATION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|), N(|x|)\bigr)$, which is exactly what the MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with (V_x, p) performs. By Proposition 22, the MARRIOTT-WATROUS AMPLIFICATION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|), N(|x|)\bigr)$ results in acceptance with probability at least

$$1 - e^{-\frac{N(|x|)}{4}} \geq 1 - e^{-\frac{\log p(|x|)}{\log e}} = 1 - \frac{1}{p(|x|)}$$

if x is in A_{yes}, and at most

$$e^{-\frac{N(|x|)}{4}} \leq e^{-\frac{\log p(|x|)}{\log e}} = \frac{1}{p(|x|)}$$

if x is in A_{no}, and the completeness and soundness follows.

The MARRIOTT-WATROUS AMPLIFICATION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|), N(|x|)\bigr)$ uses extra workspace (relative to V'_x) of $\delta_2(|x|)$ qubits for the function $\delta_2\colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $\delta_2 = 2N + \lceil \log(2N+1) \rceil + 1$. As $N = \lceil \frac{4 \log p}{\log e} \rceil$, δ_2 is clearly logarithmic with respect to p, and thus, with respect to $\frac{p}{c-s}$ also. Hence, the MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with (V_x, p) uses extra workspace (relative to V_x) of logarithmically many qubits with respect to $\frac{p}{c-s}$ also (which is determined by a function $\delta = \delta_1 + \delta_2$), as desired. ☐

Soundness error-reduction The rest of the construction is very similar to that in Subsection 5.1.

Again fix arbitrarily a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $N\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$N = \left\lceil \frac{p}{2\log(2p)} \right\rceil.$$

Fix an input x. Given the pair (V_x, p), consider the MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with $(V_x, 4p^2)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned

SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p)

Define a function $N\colon \mathbb{Z}^+ \to \mathbb{N}$ by $N = \left\lceil \frac{p}{2\log(2p)} \right\rceil$. Consider the MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with $(V_x, 4p^2)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.
Perform the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$.

Figure 12: The SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION.

by the accepting states of it. From the triplet $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}\bigr)$ and a positive integer $N(|x|)$, one constructs the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$, and performs it. The resulting procedure is called the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION, and is summarized in Figure 12.

The following lemma is proved by using the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION combined with the properties of the MILD AMPLIFICATION WITH MARRIOTT-WATROUS used for proving Lemma 26.

Lemma 29. *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and any functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}]\left(1 - \frac{1}{p}, 2^{-2p}\right).$$

Proof. Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and an input x in Σ^*. The lemma is proved by considering the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p).

First consider the MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with $(V_x, 4p^2)$. Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.

Lemma 26 and its proof based on the MILD AMPLIFICATION WITH MARRIOTT-WATROUS ensure that A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta_1, l_{\mathsf{M}}]\bigl(1 - \frac{1}{4p^2}, \frac{1}{4p^2}\bigr)$ for some function $\delta_1\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$, and this inclusion is certified by the MILD AMPLIFICATION WITH MARRIOTT-WATROUS associated with $(V_x, 4p^2)$. This in particular implies that the Hermitian operator $M'_x = \Pi'_{\mathrm{init}}(V'_x)^\dagger \Pi'_{\mathrm{acc}} V'_x \Pi'_{\mathrm{init}}$ has an eigenvalue at least $1 - \frac{1}{4(p(|x|))^2}$ if x is in A_{yes}, while all the eigenvalues of M'_x are at most $\frac{1}{4(p(|x|))^2}$ if x is in A_{no}.

Now consider the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$, which is exactly what the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p) performs. By Proposition 19, the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$ results in acceptance with probability at least

$$\left(1 - \frac{1}{4(p(|x|))^2}\right)^{2\,N(|x|)} > \left(1 - \frac{1}{4(p(|x|))^2}\right)^{\frac{p(|x|)}{\log(2\,p(|x|))} + 2} > 1 - \frac{1}{p(|x|)}$$

SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION associated with (V_x, p)

Define a function $N\colon \mathbb{Z}^+ \to \mathbb{N}$ by $N = \lceil \frac{p}{2\log p} \rceil$. Consider the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.
Perform the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$.

Figure 13: The SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION.

if x is in A_{yes}, and at most

$$\left(\frac{1}{4(p(|x|))^2}\right)^{2\,N(|x|)} \leq \left[\left(\frac{1}{2\,p(|x|)}\right)^{\frac{p(|x|)}{\log(2\,p(|x|))}}\right]^2 = 2^{-2\,p(|x|)}$$

if x is in A_{no}, and the completeness and soundness follows.

The AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$ uses extra workspace (relative to V'_x) of $\delta_2(|x|)$ qubits for the function $\delta_2\colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $\delta_2 = \lceil \log(2N+1) \rceil$. As $N = \lceil \frac{p}{2\log(2p)} \rceil$, δ_2 is clearly logarithmic with respect to p, and thus, with respect to $\frac{p}{c-s}$ also. Hence, the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p) uses extra workspace (relative to V_x) of logarithmically many qubits with respect to $\frac{p}{c-s}$ also (which is determined by a function $\delta = \delta_1 + \delta_2$), as desired. $\square$

Space-efficient error reduction based on hybrid construction Again fix arbitrarily a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $N\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$N = \left\lceil \frac{p}{2\log p} \right\rceil.$$

Fix an input x. Given the pair (V_x, p), consider the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it. From the triplet $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}\bigr)$ and a positive integer $N(|x|)$, one constructs the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$, and performs it. The resulting procedure is called the SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION, and is summarized in Figure 13.

Now Theorem 1, the main theorem of this paper, is ready to be proved by using the SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION combined with the properties of the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION used for proving Lemma 29.

Proof of Theorem 1 (via the hybrid construction of phase estimation and Marriott-Watrous). Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x\in\Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and an input x in Σ^*. The theorem is proved by considering the SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION associated with (V_x, p).

First consider the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.

Lemma 29 and its proof ensure that A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}+\delta_1, l_{\mathsf{M}}]\bigl(1-\frac{1}{p}, 2^{-2p}\bigr)$ for some function $\delta_1 \colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$, and this inclusion is certified by the SOUNDNESS ERROR REDUCTION WITH HYBRID CONSTRUCTION associated with (V_x, p). This in particular implies that the Hermitian operator $M'_x = \Pi'_{\mathrm{init}}(V'_x)^\dagger \Pi'_{\mathrm{acc}} V'_x \Pi'_{\mathrm{init}}$ has an eigenvalue at least $1-\frac{1}{p(|x|)}$ if x is in A_{yes}, while all the eigenvalues of M'_x are at most $2^{-2\,p(|x|)}$ if x is in A_{no}.

Now consider the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$, which is exactly what the SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION associated with (V_x, p) performs. By Proposition 21, the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$ results in acceptance with probability at least

$$1-\left(\frac{1}{p(|x|)}\right)^{2\,N(|x|)} \geq 1-\left(2^{-\log p(|x|)}\right)^{\frac{p(|x|)}{\log p(|x|)}} = 1-2^{-\,p(|x|)}$$

if x is in A_{yes}, and at most

$$1-\left(1-2^{-2\,p(|x|)}\right)^{2\,N(|x|)} < 1-\left(1-2^{-2\,p(|x|)}\right)^{\frac{p(|x|)}{\log p(|x|)}+2} < 2^{-\,p(|x|)}$$

if x is in A_{no}, and the completeness and soundness follows.

The OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$ uses extra workspace (relative to V'_x) of $\delta_2(|x|)$ qubits for the function $\delta_2 \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $\delta_2 = \lceil \log(2N+1) \rceil$. As $N = \bigl\lceil \frac{p}{2\log p} \bigr\rceil$, δ_2 is clearly logarithmic with respect to p, and thus, with respect to $\frac{p}{c-s}$ also. Hence, the SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION associated with (V_x, p) uses extra workspace (relative to V_x) of logarithmically many qubits with respect to $\frac{p}{c-s}$ also (which is determined by a function $\delta = \delta_1 + \delta_2$), as desired. □

A straightforward calculation shows that the SPACE-EFFICIENT ERROR REDUCTION BASED ON HYBRID CONSTRUCTION associated with (V_x, p) uses $O\bigl(\frac{1}{c-s} \cdot \frac{p^2}{\log p}\bigr)$ calls of V_x and its inverse.

5.3 Exactly implementable construction based on random guess

The third proof is via the exactly implementable construction based on random guess.

Mild completeness amplification with a guess Fix a function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$ arbitrarily, and let $l, C \colon \mathbb{Z}^+ \to \mathbb{N}$ be functions defined by

$$l = \left\lceil \frac{1}{2} \log \frac{p}{(c-s)^2} \right\rceil, \quad C = \lceil 2^l c \rceil.$$

Fix an input x and a positive integer k in $\{1, \ldots, 2^{l(|x|)}\}$. Given the triplet $(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}})$ and the integer k, one first constructs the ADDITIVE ADJUSTMENT PROCEDURE associated with $\bigl(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}}, l(|x|), k\bigr)$, if k is at least $C(|x|)$ (and automatically rejects otherwise so that no k can result in a good guess at the acceptance probability when the actual value of it is unallowably small). Let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\mathrm{acc},k}$ be the projection onto the subspace spanned by the accepting states of it. Next, from the triplet $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}\bigr)$, one constructs the REFLECTION PROCEDURE associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}\bigr)$, and performs it. The resulting procedure is called the MILD COMPLETENESS AMPLIFICATION WITH GUESS k, and is summarized as in Figure 14.

From the properties of the ADDITIVE ADJUSTMENT PROCEDURE and the REFLECTION PROCEDURE (Propositions 24 and 25), one can show the following lemma.

MILD COMPLETENESS AMPLIFICATION WITH GUESS k associated with (V_x, p)

Define functions l and C by $l = \left\lceil \frac{1}{2} \log \frac{p}{(c-s)^2} \right\rceil$ and $C = \lceil 2^l c \rceil$. Let Π_{init} and Π_{acc} be the projections onto the subspaces spanned by the legal initial states and the accepting states, respectively, in the verification with V_x. Given an integer k in $\{1, \dots, 2^{l(|x|)}\}$ as a guess, consider the ADDITIVE ADJUSTMENT PROCEDURE associated with $(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}}, l(|x|), k)$. Let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\mathrm{acc},k}$ be the projection onto the subspace spanned by the accepting states of it.

Reject if $k < C(|x|)$, and continue otherwise by performing the REFLECTION PROCEDURE associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}\bigr)$.

Figure 14: The MILD COMPLETENESS AMPLIFICATION WITH GUESS k.

Lemma 30. *Given functions $l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Then, for any function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and for every x in Σ^*, letting $l = \left\lceil \frac{1}{2} \log \frac{p}{(c-s)^2} \right\rceil$, the following properties hold:*

(Completeness) *If x is in A_{yes}, there exists an integer k in $\{1, \dots, 2^{l(|x|)}\}$ as a guess such that the* MILD COMPLETENESS AMPLIFICATION WITH GUESS *k associated with (V_x, p) results in acceptance with probability at least $1 - \frac{(c(|x|) - s(|x|))^2}{p(|x|)}$.*

(Soundness) *If x is in A_{no}, for any integer k in $\{1, \dots, 2^{l(|x|)}\}$ as a guess, the* MILD COMPLETENESS AMPLIFICATION WITH GUESS *k associated with (V_x, p) results in acceptance with probability at most $1 - \bigl(c(|x|) - s(|x|)\bigr)^2$.*

Proof. Let $C \colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by $C = \lceil 2^l c \rceil$, and let Π_{init} and Π_{acc} be the projections onto the subspaces spanned by the legal initial states and the accepting states, respectively, in the verification with V_x. For the ADDITIVE ADJUSTMENT PROCEDURE associated with $(V_x, \Pi_{\mathrm{init}}, \Pi_{\mathrm{acc}}, l(|x|), k)$, let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\mathrm{acc},k}$ be the projection onto the subspace spanned by the accepting states of it.

First suppose that x is in A_{yes}. The Hermitian operator $M_x = \Pi_{\mathrm{init}} V_x^\dagger \Pi_{\mathrm{acc}} V_x \Pi_{\mathrm{init}}$ in this case has an eigenvalue λ_x that is at least $c(|x|)$.

Fix $k = \lceil 2^{l(|x|)} \lambda_x \rceil$ in $\{C(|x|), \dots, 2^{l(|x|)}\}$.

By Proposition 24, the Hermitian operator $M'_{x,k} = \Pi'_{\mathrm{init}} \bigl(V'_{x,k}\bigr)^\dagger \Pi'_{\mathrm{acc},k} V'_{x,k} \Pi'_{\mathrm{init}}$ must have an eigenvalue

$$\lambda'_{x,k} = \frac{1}{2} - \frac{1}{2}\left(\frac{k}{2^{l(|x|)}} - \lambda_x\right),$$

which must satisfy that

$$\frac{1}{2} - \frac{c(|x|) - s(|x|)}{2\sqrt{p(|x|)}} \leq \frac{1}{2} - 2^{-(l(|x|)+1)} < \lambda'_{x,k} \leq \frac{1}{2}$$

for $k = \lceil 2^{l(|x|)} \lambda_x \rceil$ in $\{C(|x|), \dots, 2^{l(|x|)}\}$.

SOUNDNESS ERROR REDUCTION WITH GUESS k associated with (V_x, p)

Define functions l and N by $l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil$ and $N = \left\lceil \frac{p}{2(c-s)^2} \right\rceil$. Given an integer k in $\{1, \ldots, 2^{l(|x|)}\}$, consider the MILD COMPLETENESS AMPLIFICATION WITH GUESS k associated with $(V_x, 6p)$. Let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\mathrm{acc},k}$ be the projection onto the subspace spanned by the accepting states of it.
Perform the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}, N(|x|)\bigr)$.

Figure 15: The SOUNDNESS ERROR REDUCTION WITH GUESS k.

Hence, by Proposition 25, the REFLECTION PROCEDURE associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}\bigr)$ results in acceptance with probability at least

$$1 - \left(\frac{k}{2^{l(|x|)}} - \lambda_x \right)^2 > 1 - 2^{-2\,l(|x|)} \geq 1 - \frac{\bigl(c(|x|) - s(|x|)\bigr)^2}{p(|x|)},$$

which proves the completeness.

Now suppose that x is in A_{no}, which implies that all the eigenvalues of M_x are at most $s(|x|)$. It follows from Proposition 24 that, for any k in $\{C(|x|), \ldots, 2^{l(|x|)}\}$, all the eigenvalues of $M'_{x,k}$ are at most

$$\frac{1}{2} - \frac{1}{2}\left(\frac{k}{2^{l(|x|)}} - s(|x|) \right) \leq \frac{1}{2} - \frac{1}{2}\left(\frac{C(|x|)}{2^{l(|x|)}} - s(|x|) \right) \leq \frac{1}{2} - \frac{1}{2}\bigl(c(|x|) - s(|x|)\bigr).$$

Therefore, Proposition 25 ensures that, for any k in $\{C(|x|), \ldots, 2^{l(|x|)}\}$, the REFLECTION PROCEDURE associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}\bigr)$ results in acceptance with probability at most

$$1 - \bigl(c(|x|) - s(|x|)\bigr)^2.$$

As it always rejects when k is less than $C(|x|)$, the MILD COMPLETENESS AMPLIFICATION WITH GUESS k associated with (V_x, p) results in acceptance with probability at most $1 - \bigl(c(|x|) - s(|x|)\bigr)^2$ for any k in $\{1, \ldots, 2^{l(|x|)}\}$, and the soundness follows. ☐

Soundness error reduction with a guess Again fix a function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, arbitrarily. Let $l, N \colon \mathbb{Z}^+ \to \mathbb{N}$ be functions defined by

$$l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil, \quad N = \left\lceil \frac{p}{2(c-s)^2} \right\rceil.$$

Fix an input x and an integer k in $\{1, \ldots, 2^{l(|x|)}\}$. Given the pair (V_x, p) and the integer k, consider the MILD COMPLETENESS AMPLIFICATION WITH GUESS k associated with $(V_x, 6p)$. As before, let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\mathrm{acc},k}$ be the projection onto the subspace spanned by the accepting states of it. From the triplet $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}\bigr)$ and a positive integer $N(|x|)$, one constructs the AND-TYPE REPETITION PROCEDURE associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}, N(|x|)\bigr)$, and performs it. The resulting procedure is called the SOUNDNESS ERROR REDUCTION WITH GUESS k, and is summarized in Figure 15.

From the properties of the AND-TYPE REPETITION PROCEDURE and the MILD COMPLETENESS AMPLIFICATION WITH GUESS k (Proposition 19 and Lemma 30), one can show the following lemma.

Lemma 31. *Given functions $l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Then, for any function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and for every x in Σ^*, letting $l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil$, the following properties hold:*

(Completeness) *If x is in A_{yes}, there exists an integer k in $\{1, \ldots, 2^{l(|x|)}\}$ as a guess such that the* Soundness Error-Reduction with Guess *k associated with (V_x, p) results in acceptance with probability at least $\frac{1}{2}$.*

(Soundness) *If x is in A_{no}, for any integer k in $\{1, \ldots, 2^{l(|x|)}\}$ as a guess, the* Soundness Error-Reduction with Guess *k associated with (V_x, p) results in acceptance with probability at most $2^{-p(|x|)}$.*

Proof. Let $C \colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by $C = \lceil 2^l c \rceil$, and let Π_{init} and Π_{acc} be the projections onto the subspaces spanned by the legal initial states and the accepting states, respectively, in the verification with V_x. For the Mild Completeness Amplification with Guess k associated with $(V_x, 6p)$, let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\mathrm{acc},k}$ be the projection onto the subspace spanned by the accepting states of it. Then, for a function $N \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $N = \left\lceil \frac{p}{2(c-s)^2} \right\rceil$ and for the AND-Type Repetition Procedure associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}, N(|x|)\bigr)$, let $V''_{x,k}$ be the unitary transformation induced by it, let Π''_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi''_{\mathrm{acc},k}$ be the projection onto the subspace spanned by the accepting states of it.

First suppose that x is in A_{yes}. The Hermitian operator $M_x = \Pi_{\mathrm{init}} V_x^\dagger \Pi_{\mathrm{acc}} V_x \Pi_{\mathrm{init}}$ in this case has an eigenvalue λ_x that is at least $c(|x|)$.

Fix $k = \lceil 2^{l(|x|)} \lambda_x \rceil$ in $\{C(|x|), \ldots, 2^{l(|x|)}\}$.

By Lemma 30, the Hermitian operator $M'_{x,k} = \Pi'_{\mathrm{init}} \bigl(V'_{x,k}\bigr)^\dagger \Pi'_{\mathrm{acc},k} V'_{x,k} \Pi'_{\mathrm{init}}$ must have an eigenvalue

$$\lambda'_{x,k} > 1 - \frac{\bigl(c(|x|) - s(|x|)\bigr)^2}{6\,p(|x|)}$$

for $k = \lceil 2^{l(|x|)} \lambda_x \rceil$ in $\{C(|x|), \ldots, 2^{l(|x|)}\}$. Hence, by Proposition 19, the AND-Type Repetition Procedure associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}, N(|x|)\bigr)$ results in acceptance with probability at least

$$\left[1 - \frac{\bigl(c(|x|) - s(|x|)\bigr)^2}{6\,p(|x|)}\right]^{2\,N(|x|)} \geq \left[1 - \frac{\bigl(c(|x|) - s(|x|)\bigr)^2}{6\,p(|x|)}\right]^{\frac{p(|x|)}{(c(|x|)-s(|x|))^2}+2} > \frac{1}{2},$$

which proves the completeness.

Now suppose that x is in A_{no}, which implies that all the eigenvalues of M_x are at most $s(|x|)$. It follows from Lemma 30 that, for any k in $\{C(|x|), \ldots, 2^{l(|x|)}\}$, all the eigenvalues of $M'_{x,k}$ are at most

$$1 - \bigl(c(|x|) - s(|x|)\bigr)^2.$$

From Proposition 19, this implies that, for any k in $\{C(|x|), \ldots, 2^{l(|x|)}\}$, the AND-Type Repetition Procedure associated with $\bigl(V'_{x,k}, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc},k}, N(|x|)\bigr)$ results in acceptance with probability at most

$$\left[1 - \bigl(c(|x|) - s(|x|)\bigr)^2\right]^{2\,N(|x|)} \leq \left[1 - \bigl(c(|x|) - s(|x|)\bigr)^2\right]^{\frac{p(|x|)}{(c(|x|)-s(|x|))^2}} < e^{-p(|x|)} < 2^{-p(|x|)}.$$

As it always rejects when k is less than $C(|x|)$, the Soundness Error Reduction with Guess k associated with (V_x, p) results in acceptance with probability at most $2^{-p(|x|)}$ for any k in $\{1, \ldots, 2^{l(|x|)}\}$, and the soundness follows. ∎

SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS associated with (V_x, p)

Define a function l by $l = \lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \rceil$.
Pick an integer k from $\{1, \ldots, 2^{l(|x|)}\}$ uniformly at random and perform the SOUNDNESS ERROR REDUCTION WITH GUESS k associated with (V_x, p).

Figure 16: The SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS.

Soundness error reduction with a random guess Again fix arbitrarily a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $l\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by

$$l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil.$$

Fix an input x. Given the pair (V_x, p), consider choosing an integer k from $\{1, \ldots, 2^{l(|x|)}\}$ uniformly at random, and then performing the SOUNDNESS ERROR REDUCTION WITH GUESS k associated with (V_x, p). The resulting procedure is called the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS and is summarized in Figure 16.

The following lemma is proved by using the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS combined with the properties of the SOUNDNESS ERROR REDUCTION WITH GUESS k stated in Lemma 31.

Lemma 32. *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and any functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$ and $\frac{c-s}{4\sqrt{6p}} > 2^{-p}$ (which in particular holds when $p > 2 \log \frac{4\sqrt{3}}{c-s}$), there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}]\left(\frac{c-s}{4\sqrt{6p}}, 2^{-p}\right).$$

Proof. Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ satisfying $\frac{c-s}{4\sqrt{6p}} > 2^{-p}$ and an input x in Σ^*. The lemma is proved by considering the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS associated with (V_x, p).

Lemma 31 ensures that, if x is in A_{yes}, the SOUNDNESS ERROR REDUCTION WITH GUESS k associated with (V_x, p) results in acceptance with probability at least $\frac{1}{2}$ for some k in $\{1, \ldots, 2^{l(|x|)}\}$, while if x is in A_{no}, it results in acceptance with probability at most $2^{-p(|x|)}$ for any k in $\{1, \ldots, 2^{l(|x|)}\}$. Hence, obviously from its construction, the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS associated with (V_x, p) results in acceptance with probability at least

$$2^{-l(|x|)} \cdot \frac{1}{2} > \frac{c(|x|) - s(|x|)}{2\sqrt{6\,p(|x|)}} \cdot \frac{1}{2} = \frac{c(|x|) - s(|x|)}{4\sqrt{6\,p(|x|)}}$$

if x is in A_{yes}, and at most $2^{-p(|x|)}$ if x is in A_{no}. This shows the completeness and soundness.

From the structures of the ADDITIVE ADJUSTMENT PROCEDURE, REFLECTION PROCEDURE, and the AND-TYPE REPETITION PROCEDURE, the SOUNDNESS ERROR REDUCTION WITH GUESS k associated with (V_x, p) uses extra workspace (relative to V_x) of $\delta_1(|x|)$ qubits for the function $\delta_1\colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $\delta_1 = l + \lceil \log(2N+1) \rceil + 1$, where $l = \lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \rceil$ and $N = \lceil \frac{p}{2(c-s)^2} \rceil$. Hence, δ_1 is clearly logarithmic with respect to $\frac{p}{c-s}$. Therefore, the SOUNDNESS ERROR-REDUCTION WITH RANDOM GUESS associated with (V_x, p)

SPACE-EFFICIENT AMPLIFICATION BASED ON RANDOM GUESS associated with (V_x, p)

Define functions q and N by $q = \lceil 2(p + \log \frac{6p}{c-s} + 1) \rceil$ and $N = \left\lceil \frac{2\sqrt{6q}}{c-s} \cdot p \right\rceil$. Consider the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS associated with (V_x, q). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.
Perform the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$.

Figure 17: The SPACE-EFFICIENT AMPLIFICATION BASED ON RANDOM GUESS.

uses extra workspace (relative to V_x) of logarithmically many qubits with respect to $\frac{p}{c-s}$ also (which is determined by a function $\delta = \delta_1 + 2l$, as the random guess may be implemented by preparing a sufficiently many number of EPR pairs and using each half of them), as desired. $\square$

Space-efficient amplification based on a random guess Again fix arbitrarily a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$. Let $q, N\colon \mathbb{Z}^+ \to \mathbb{N}$ be functions defined by

$$q = \left\lceil 2\left(p + \log \frac{6p}{c-s} + 1\right)\right\rceil, \quad N = \left\lceil \frac{2\sqrt{6q}}{c-s} \cdot p \right\rceil.$$

Fix an input x. Given the pair (V_x, p), consider the SOUNDNESS ERROR-REDUCTION WITH RANDOM GUESS associated with (V_x, q). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it. From the triplet $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}\bigr)$ and a positive integer $N(|x|)$, one constructs the OR-TYPE REPETITION PROCEDURE associated with $\bigl(V'_x, \Pi'_{\mathrm{init}}, \Pi'_{\mathrm{acc}}, N(|x|)\bigr)$, and performs it. The resulting procedure is called the SPACE-EFFICIENT AMPLIFICATION BASED ON RANDOM GUESS and is summarized in Figure 17.

Now Theorem 1, the main theorem of this paper, is ready to be proved by using the SPACE-EFFICIENT AMPLIFICATION BASED ON RANDOM GUESS combined with the properties of the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS used for proving Lemma 32.

Proof of Theorem 1 (via the exactly implementable construction based on a random guess) . Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s)$, and let $V = \{V_x\}_{x\in\Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and an input x in Σ^*. Let The theorem is proved by considering the SPACE-EFFICIENT AMPLIFICATION BASED ON RANDOM GUESS associated with (V_x, p).

Let $q\colon \mathbb{Z}^+ \to \mathbb{N}$ be the function defined by $q = \lceil 2(p + \log \frac{6p}{c-s} + 1)\rceil$. First consider the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS associated with (V_x, q). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.

As the function q satisfies that $q > 2\log\frac{4\sqrt{3}}{c-s}$, and thus, that $\frac{c-s}{4\sqrt{6q}} > 2^{-q}$, Lemma 32 and its proof ensure that A is in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta_1, l_{\mathsf{M}}]\bigl(\frac{c-s}{4\sqrt{6q}}, 2^{-q}\bigr)$ for some function $\delta_1\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{q}{c-s}$ (and thus, with respect to $\frac{p}{c-s}$), and this inclusion is certified by the SOUNDNESS ERROR REDUCTION WITH RANDOM GUESS associated with (V_x, q). This in particular implies that the Hermitian operator $M'_x = \Pi'_{\mathrm{init}}(V'_x)^\dagger \Pi'_{\mathrm{acc}} V'_x \Pi'_{\mathrm{init}}$ has an eigenvalue at least $\frac{c(|x|)-s(|x|)}{4\sqrt{6\,q(|x|)}}$ if x is in A_{yes}, while all the eigenvalues of M'_x are at most $2^{-\,q(|x|)}$ if x is in A_{no}.

Now consider the OR-TYPE REPETITION PROCEDURE associated with $\big(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\big)$, which is exactly what the SPACE-EFFICIENT ERROR REDUCTION BASED ON RANDOM GUESS associated with (V_x, p) performs. By Proposition 21, the OR-TYPE REPETITION PROCEDURE associated with $\big(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\big)$ results in acceptance with probability at least

$$
\begin{aligned}
1 - &\left(1 - \frac{c(|x|) - s(|x|)}{4\sqrt{6\,q(|x|)}}\right)^{2\,N(|x|)} \\
&\geq 1 - \left(1 - \frac{c(|x|) - s(|x|)}{4\sqrt{6\,q(|x|)}}\right)^{\frac{4\sqrt{6\,q(|x|)}}{c(|x|)-s(|x|)} \cdot p(|x|)} > 1 - e^{-\,p(|x|)} > 1 - 2^{-\,p(|x|)}
\end{aligned}
$$

if x is in A_{yes}, and at most

$$
\begin{aligned}
1 - \left(1 - 2^{-\,q(|x|)}\right)^{2\,N(|x|)} &< 2^{-\,q(|x|)+1} \cdot N(|x|) \\
&< 2^{-\,p(|x|) - \log \frac{6\,p(|x|)}{c(|x|)-s(|x|)}} \cdot 2^{-\frac{1}{2}\,q(|x|)} \cdot \left(\frac{2\sqrt{6\,q(|x|)}}{c(|x|) - s(|x|)} \cdot p(|x|) + 1\right) \\
&< 2^{-\,p(|x|)} \cdot \frac{c(|x|) - s(|x|)}{6\,p(|x|)} \cdot \frac{1}{\sqrt{q(|x|)}} \cdot \left(\frac{6\sqrt{q(|x|)}}{c(|x|) - s(|x|)} \cdot p(|x|)\right) \\
&< 2^{-\,p(|x|)}
\end{aligned}
$$

if x is in A_{no}, where the third inequality uses the fact that $2\sqrt{6} + 1 < 6$, and the completeness and soundness follows.

The OR-TYPE REPETITION PROCEDURE associated with $\big(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\big)$ uses extra workspace (relative to V'_x) of $\delta_2(|x|)$ qubits for the function $\delta_2 \colon \mathbb{Z}^+ \to \mathbb{N}$ defined by $\delta_2 = \lceil \log(2N + 1) \rceil$. As $N = \left\lceil \frac{2\sqrt{6q}}{c-s} \right\rceil$ and $q = \left\lceil 2\big(p + \log \frac{6p}{c-s} + 1\big) \right\rceil$, δ_2 is clearly logarithmic with respect to $\frac{p}{c-s}$. Hence, the SPACE-EFFICIENT ERROR REDUCTION BASED ON RANDOM GUESS associated with (V_x, p) uses extra workspace (relative to V_x) of logarithmically many qubits with respect to $\frac{p}{c-s}$ also (which is determined by a function $\delta = \delta_1 + \delta_2$), as desired. □

Acknowledgements

BF and CYL are supported by the Department of Defense. HK and HN are supported by the Grant-in-Aid for Scientific Research (A) No. 24240001 of the Japan Society for the Promotion of Science. TM is supported by the Program to Disseminate Tenure Tracking System of the Ministry of Education, Culture, Sports, Science and Technology in Japan, the Grant-in-Aid for Scientific Research on Innovative Areas No. 15H00850 of the Ministry of Education, Culture, Sports, Science and Technology in Japan, and the Grant-in-Aid for Young Scientists (B) No. 26730003 of the Japan Society for the Promotion of Science. HN is also supported by the Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009 of the Ministry of Education, Culture, Sports, Science and Technology in Japan, which HK is also grateful to. HN further acknowledges support from the Grant-in-Aid for Scientific Research (C) No. 25330012 of the Japan Society for the Promotion of Science.

References

[AF98] ANDRIS AMBAINIS AND RŪSIŅŠ FREIVALDS. 1-way quantum finite automata: strengths, weaknesses and generalizations. In *39th Annual Symposium on Foundations of Computer Science*, pages 332–341, 1998.

[Ben89] CHARLES H. BENNETT. Time/space trade-offs for reversible computation. *SIAM Journal on Computing*, 18(4):766–776, 1989.

[DN06] CHRISTOPHER M. DAWSON AND MICHAEL A. NIELSEN. The Solovay-Kitaev algorithm. *Quantum Information and Computation*, 6(1):081–095, 2006.

[FL16a] BILL FEFFERMAN AND CEDRIC LIN. Quantum Merlin Arthur with exponentially small gap. arXiv.org e-Print archive, arXiv:1601.01975 [quant-ph], 2016.

[FL16b] BILL FEFFERMAN AND CEDRIC YEN-YU LIN. A complete characterization of unitary quantum space. arXiv.org e-Print archive, arXiv:1604.01384 [quant-ph], 2016.

[Gro96] LOV K. GROVER. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, 1996.

[IKW12] TSUYOSHI ITO, HIROTADA KOBAYASHI, AND JOHN WATROUS. Quantum interactive proofs with weak error bounds. In *ITCS '12, Proceedings of the 2012 ACM Conference on Innovations in Theoretical Computer Science*, pages 266–275, 2012.

[JKMW10] RICHARD JOZSA, BARBARA KRAUS, AKIMASA MIYAKE, AND JOHN WATROUS. Matchgate and space-bounded quantum computations are equivalent. *Proceedings of the Royal Society A*, 466(2115):809–830, 2010.

[JKNN12] STEPHEN P. JORDAN, HIROTADA KOBAYASHI, DANIEL NAGAJ, AND HARUMICHI NISHIMURA. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):0461–0471, 2012.

[Kit97] A. YU. KITAEV. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[KLGN15] HIROTADA KOBAYASHI, FRANÇOIS LE GALL, AND HARUMICHI NISHIMURA. Stronger methods of making quantum interactive proofs perfectly complete. *SIAM Journal on Computing*, 44(2):243–289, 2015.

[KSV02] ALEXEI YU. KITAEV, ALEXANDER H. SHEN, AND MIKHAIL N. VYALYI. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[KW00] ALEXEI KITAEV AND JOHN WATROUS. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[MW05] CHRIS MARRIOTT AND JOHN WATROUS. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[NC00] MICHAEL A. NIELSEN AND ISAAC L. CHUANG. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NW16] ANAND NATARAJAN AND XIAODI WU. Private communication, January 2016.

[NWZ09] DANIEL NAGAJ, PAWEL WOCJAN, AND YONG ZHANG. Fast amplification of QMA. *Quantum Information and Computation*, 9(11–12):1053–1068, 2009.

[TD02] BARBARA M. TERHAL AND DAVID P. DIVINCENZO. Classical simulation of noninteracting-fermion quantum circuits. *Physical Review A*, 65:article 032325, 2002.

[TS13] AMNON TA-SHMA. Inverting well conditioned matrices in quantum logspace. In *STOC'13, Proceedings of the 2013 ACM Symposium on Theory of Computing*, pages 881–890, 2013.

[Val02] LESLIE G. VALIANT. Quantum circuits that can be simulated classically in polynomial time. *SIAM Journal on Computing*, 31(4):1229–1254, 2002.

[vMW12] DIETER VAN MELKEBEEK AND THOMAS WATSON. Time-space efficient simulations of quantum computations. *Theory of Computing*, 8:1–51 (article 1), 2012.

[Wat99] JOHN WATROUS. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999.

[Wat01] JOHN WATROUS. Quantum simulations of classical random walks and undirected graph connectivity. *Journal of Computer and System Sciences*, 62(2):376–391, 2001.

[Wat03] JOHN WATROUS. On the complexity of simulating space-bounded quantum computations. *Computational Complexity*, 12(1–2):48–84, 2003.

[Wat09a] JOHN WATROUS. Quantum computational complexity. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. Springer New York, 2009.

[Wat09b] JOHN WATROUS. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

[Wil13] MARK M. WILDE. *Quantum Information Theory*. Cambridge University Press, 2013.